LAUREA AMMATTIKORKEAKOULU Uuden edellä

Viranomaisyksikön turvallisuusjohtamisen tason todentaminen KATAKRIn avulla

Kojo, Jussi

2013 Leppävaara

Laurea-ammattikorkeakoulu
Leppävaara

Viranomaisyksikön turvallisuusjohtamisen tason todentaminen KATAKRIn avulla

Jussi Kojo
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Marraskuu, 2013

Sisällys

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Turvallisuusalan koulutusohjelma

Jussi Kojo

Viranomaisyksikön turvallisuusjohtamisen tason todentaminen KATAKRIn avulla

Vuosi 2013 Sivumäärä 53

Tämän opinnäytetyön tavoitteena oli todentaa turvallisuusjohtamisen taso suomalaisen turvallisuusorganisaation viranomaisyksikössä. Todentaminen suoritettiin Kansallisen turvallisuusauditointikriteeristö KATAKRIn avulla. Tavoitteena oli myös selvittää, soveltuuko KATAKRI viranomaisyksikköön. Kyseessä ei ollut virallinen KATAKRI-auditointi, vaikka todentamisessa käytettiin varsinaista turvallisuusauditointiprosessia. Turvallisuuden arviointi rajattiin myös koskemaan vain kohteen hallinnollista turvallisuutta eli turvallisuuden johtamista ja sen yhtä suojaustasovaatimusta, korotettu taso III:sta.

Opinnäytetyö oli kvalitatiivinen eli laadullinen tutkimus, jonka tutkimusmenetelminä toimivat dokumenttianalyysit, haastattelut ja havainnointi. Kvalitatiivisena tutkimuslajina käytettiin hermeneuttista menetelmää. Ensisijaisena tiedonkeruumenetelmänä käytettiin turvallisuusdokumenttien tarkastelua, toisena KATAKRIn kysymyssarjaan perustuvia, strukturoituja haastatteluja ja kolmantena havainnointia, jossa seurattiin käytännössä yksikön turvallisuusjohtamisen toimintaa.

Opinnäytetyö alkaa tutkimuksen teoreettisella viitekehyksellä ja turvallisuusauditoinnin teorialla. Tämän jälkeen on vuorossa kohteen auditointi, missä kuvaillaan käyty auditointiprosessi sekä laadittu tulosanalyysi. Analyysin perusteella esitetään kohteelle kooste turvallisuusjohtamisen kehittämisehdotuksista. Näitä kohde voi tarvittaessa käyttää hyödykseen parantaakseen suojaustasoaan ja hallinnollista turvallisuuttaan tai muodostaakseen turvallisuuden kehittämissuunnitelman. Turvallisuusjohtamisen todentamisen tulokset kirjataan myös tämän raportin liitteeksi.

Tämän opinnäytetyön myötä saatiin kohteen turvallisuusjohtamisen tasosta raportti, joka perustuu KATAKRIn security-näkökulmaan. KATAKRI tuotiin tutkimuksessa viranomaisympäristöön, jossa sen soveltaminen oli osittain haastavaa. Suojaustasovaatimuksia tuli soveltaa saatuihin havaintoihin ja kohteen toimintaympäristöön. KATAKRI turvallisuuden kehittämisen työkaluna ei ollut yksikölle ennestään tuttu. Vähäisen tunnettavuuden myötä syntyi autenttisuutta erityisesti haastattelu- ja havainnointiprosesseihin. Mikäli auditointi olisi toteutettu pelkästään dokumentaatioihin ja niihin nojautuviin tietoihin, olisi suojaustasojen todentaminen jäänyt vaatimattomaksi.

Yksikölle toteutettu turvallisuusauditointi toimi yksikölle myös esiauditointina. Mikäli yksikölle suoritettaisiin virallinen KATAKRIn mukainen auditointi, tämän auditointiraportin avulla siihen kyettäisiin paremmin valmistautumaan. Auditointiraportin tulosanalyysin perusteella voidaan todeta, että auditoitavan kohteen turvallisuusjohtamisen taso ei pystynyt saavuttamaan KATAKRIn korotetun tason vaatimusta hallinnollisesta turvallisuudesta. Kohteen suojaustasovaatimukset täyttyivät enintään KATAKRIn perustason osalta.

Asiasanat: Turvallisuusjohtaminen, hallinnollinen turvallisuus, riskienhallinta, Kansallinen turvallisuusauditointikriteeristö, auditointi

Laurea University of Applied Sciences **Abstract**
Leppävaara
Bachelor's Degree Programme in Security Management

Jussi Kojo

Authentication of security management level in a Finnish authority unit using National Security Auditing Criteria

Year 2013 Pages 53

The main objective of this thesis was to authenticate the security management level in the Finnish authority unit. Authentication was performed using the National Security Auditing Criteria (Kansallinen turvallisuusauditointikriteeristö ie KATAKRI). The other objective was to examine what type of usability National Security Auditing Criteria have in such an authority unit. This was not an official audit in the National Security Auditing Criteria, even if the verification was adapted from the actual security audit process. Security assessment was also limited only to the administrative security ie security management and its requirements for the increased level (III).

This thesis was a qualitative research project, the research methods of which were document analysis, interviews and observation. The hermeneutical method was used as the qualitative research genre. The primary data collection method was the review of security documents, the second method was structured interviews with questions based on the National Security Auditing Criteria and the third method was observation, in practice monitoring the security management activities of the target unit.

The initial section of this thesis consists of the theoretical framework of research and the theory of security audits. Those are followed by the audit of the object, describing the whole audit process and showing the development of the result analysis. The results were drawn up on the result analysis that formed the basis for a summary of developments to the security management. If necessary, these developments can be used by the object to improve their level of requirements and administrative security or to form a development plan for security. The results of security management were also recorded in this report as an appendix.

As a result of this thesis project a comprehensive, security-perspective report on security management about the unit was obtained. Importing the National Security Auditing Criteria to the authorities' environment seemed to be highly challenging at first. However, time by time the author learned how to apply observations to the requirement levels of National Security Auditing Criteria and to the operating environment. National Security Auditing Criteria as a tool was not already familiar to the unit. However, low awareness could create some authenticity to processes of interviews and observations. If the audit should be carried out exclusively with documentation and its information, would authentication of requirement levels would be inadequate.

This security audit formed as a pre-audit for the unit. If the unit carried out the official National Security Auditing Criteria's audit process, this audit report could help to prepare for it considerably better. Based on the result analysis of the audit report it can be stated that the security management level of the authority unit could not reach the requirements of the increased level (III) of the National Security Auditing Criteria on administrative security. However, the object reached the maximum level of requirements of the base level.

Keywords: Security management, administrative security, risk management, National Security Auditing Criteria, auditing

1 Johdanto

Tämän laadullisen opinnäytetyön tavoitteena on todentaa turvallisuusjohtamisen taso suomalaisen turvallisuusorganisaation viranomaisyksikössä. Tarkoituksena ei ole suorittaa virallista KATAKRIn auditointiprosessia. Kyseessä on esiauditointi, jossa KATAKRIn suojaustasovaatimuksia käytetään viitearvoina ja apuvälineinä turvallisuusjohtamisen todentamiseen. Tutkimuksen toimintaympäristöön kuuluvat kaikki siihen osallistuneet henkilöt, asiat, yksiköt, organisaatiot ja organisaation osat. Tämän opinnäytetyön toimintaympäristön muodostavat opinnäytetyön tekijä, opinnäytetyön ohjaaja Laurea-ammattikorkeakoulusta, opinnäytetyön kohteena oleva viranomaisyksikkö ja sen haastateltava henkilökunta sekä Kansallinen turvallisuusauditointikriteeristö.

Opinnäytetyön auditoitava kohde on Etelä-Suomessa sijaitseva turvallisuusviranomaisyksikkö, joka työllistää noin 150 henkilöä. Kohde on osa isompaa, valtakunnallista turvallisuusorganisaatiota, joka työllistää yhteensä noin 3000 henkilöä. Turvallisuusjohtamisen auditointiin asettaa erityisiä piirteitä kyseisen yksikön luokiteltavuus turvallisuuskriittiseksi organisaatioksi. Reimanin ja Oedewaldin (2008, 17) mukaan turvallisuuskriittiseksi organisaation määrittelee siihen liittyvä toiminta. Kun toimintaan sisältyy sellaisia uhkia tai vaaroja, jotka huonosti hallittuna voivat olla vahingollisia ympäristölle tai ihmisille, voi organisaatiota luonnehtia turvallisuuskriittiseksi. Tällaisen kohteen turvallisuutta tulee aina tarkastella kriittisesti, jotta sen organisaatioturvallisuutta pystyttäisiin parantamaan ja kehittämään.

Opinnäytetyö on kvalitatiivinen eli laadullinen tutkimus, jonka tutkimusmenetelminä toimivat dokumenttiaineistojen analyysi, haastattelut ja havainnointi. Kvalitatiivisena tutkimuslajina käytetään hermeneuttista menetelmää. Ensisijaisena tiedonkeruumenetelmänä käytetään yksikön turvallisuusdokumentteja ja -asiakirjoja, joista turvallisuusjohtamisen tasoa pystytään mahdollisuuksien mukaan todentamaan. Toisena tiedonkeruumenetelmänä käytetään strukturoituja haastatteluja, jonka kysymyssarjan muodostavat Kansallisen turvallisuusauditointikriteeristön hallinnollisen turvallisuuden kysymykset. Kolmantena tiedonkeruumenetelmänä toimii osallistuva havainnointi, jota suoritetaan käytännön tasolla niin, että turvallisuusjohtamisen tason todentumista pyritään mittaamaan ja tarkastelemaan osallistumalla kohteen toimintaan.

Auditointihaastattelujen, dokumenttien tarkastelun ja havainnoinnin tulokset kirjataan tämän raportin liitteeksi. Liite muodostaa yhtenäisen auditointiraportin, mistä tulee esille auditointikysymys, suojaustasovaatimus, poikkeaman tunnistaminen ja tunnistamiseen viittaavat havainnot. Tuloksista laaditaan tulosanalyysi, jonka perusteella esitetään kohteelle kooste kehittämisehdotuksista. Näitä kohde voi tarvittaessa käyttää hyödykseen parantaakseen suojaustasoaan ja hallinnollista turvallisuuttaan. Kehittämisehdotusten tarkoituksena on myös

muodostaa perustaa mahdolliseen turvallisuuden kehittämissuunnitelmaan. Kohteen identiteetti säilytetään koko tutkimuksen aikana anonyymina, joten tutkimuksen viitekehys, yksikön toimintaympäristön kuvaus sekä yksikköön kohdistuvien lakien ja asetusten esittely ovat tunnistettavuuden vuoksi osittain rajoitettu.

2 Tutkimuskysymykset, teoreettinen viitekehys ja tutkimusmenetelmät

Hirsjärven, Remeksen ja Sajavaaran (2009, 125-126) mukaan tutkimusongelmat tulee harkita ja muotoilla tarkkaan ennen varsinaisen tutkimusaineiston keräämisen aloittamista. Tutkimuskysymysten asettelu on tutkimusstrategian, tieteenfilosofian ja teoreettisen ymmärtämisen ohella yksi tutkimuksen perustoista. Tutkimuskysymykset muodostavat johtoajatuksen, jonka ympärille työ rakentuu. Tällä tutkimuksella on kaksi keskeistä tutkimusongelmaa, jonka muodostavat seuraavat tutkimuskysymykset:

1. *Mikä on tutkimuskohteen turvallisuusjohtamisen taso?*
2. *Soveltuvatko KATAKRIn suojaustasovaatimukset kohteeseen?*

Ensimmäisen tutkimusongelman, turvallisuusjohtamisen nykytilan, selvittämiseen ja kartoittamiseen käytetään tässä raportissa turvallisuusauditointia. Turvallisuusauditoinnin suorittamisessa käytetään Kansallista turvallisuusauditointikriteeristöä eli KATAKRIa. KATAKRIn asetetut suojaustasovaatimukset hallinnollisesta turvallisuudesta toimivat vertailuarvoina kohteen vallitsevaan tasoon (Puolustusministeriö 2011). Toinen tutkimusongelma, KATAKRIn soveltuvuus viranomaisyksikköön, selvitetään arvioimalla turvallisuusauditoinnin tuloksia. Tulosanalyysin perusteella pyritään arvioimaan KATAKRIn käytettävyyttä ja selvittämään myös sen hyödynnettävyyttä kohteeseen jatkossa. KATAKRIssa määritetyt suojaustasovaatimukset eivät välttämättä sovellu tutkittavalle kohteelle niiden tehokkuuden, riittävyyden tai suhteellisuuden suhteen. On myös huomioitava, että KATAKRI ei kata kaikkia organisaatioturvallisuuden osa-alueita sen security-näkökulman vuoksi. Tämän vuoksi turvallisuusjohtamista tulee tarkastella samasta aspektista. Turvallisuusjohtamisen safety-näkökulman puuttuessa esimerkiksi kohteen palo- tai työturvallisuuden johtamista ei voida ottaa huomioon tässä tutkimuksessa.

Opinnäytetyön teoreettinen viitekehys on kirjallinen osa tutkimuksesta, jonka tarkoitus on esitellä tutkimuksen teoreettinen pohja, tutkimuskysymykset sekä käytetyt tutkimusmenetelmät. Teoreettisella viitekehyksellä tuodaan esille myös aikaisempaa tutkimustietoa käsiteltävästä aiheesta (Heinonen, Keinänen & Paasonen 2013, 29-30). Viitekehyksellä tuodaan esille myös tutkijan toimenpiteet ennen tutkimusaineiston keruuta (Hirsjärvi ym. 2009, 140).

Tutkittavana ilmiönä toimiva turvallisuusjohtaminen kuuluu organisaatioturvallisuuden kokonaisuuteen. Organisaatioturvallisuuteen kuuluu kymmenen eri osa-aluetta, joita ovat henkilö-

turvallisuus, kiinteistö- ja toimitilaturvallisuus, pelastustoiminta, rikosturvallisuus, tietoturvallisuus, tuotannon ja toiminnan turvallisuus, työturvallisuus, ulkomaantoimintojen turvallisuus, ympäristöturvallisuus ja valmiussuunnittelu (Elinkeinoelämän keskusliitto 2013). Tämän tutkimuksen piiriin kuuluvat organisaatioturvallisuuden osa-alueista vain kolme security-näkökulman osa-alueista, joita ovat fyysinen turvallisuus, tietoturvallisuus ja henkilöstöturvallisuus.

Tämä opinnäytetyö on tyypiltään kvalitatiivinen eli laadullinen tutkimus. Sen lähtökohtana on sekä todellisen elämän että kohteen kokonaisvaltainen kuvaaminen. Kvalitatiivisen tutkimuksen aineisto kootaan luonnollisissa ja todellisissa tilanteissa. Tutkimuksen kvalitatiivisina tutkimusmenetelminä toimivat dokumenttianalyysit, haastattelut ja havainnointi. Dokumenttianalyysin piiriin kuuluvat kohteen valmiit aineistot, joita ovat turvallisuusdokumentaatiot ja asiakirjat. Niitä kutsutaan primaariaineistoksi, koska ne sisältävät välitöntä tietoa tutkimuskohteesta (Hirsjärvi ym 2009, 186). Tutkimuksessa käytetään myös haastatteluja, jotta saataisiin tutkimuskysymyksiin vastauksia myös niihin kysymyksiin, joita ei primaariaineistosta saatu selville. Toisaalta haastattelujen avulla saadaan myös tarvittaessa selvennettyä ja syvennettyä dokumenttianalyysista saatuja tietoja (Hirsjärvi ym. 2009, 205). Havainnoinnin perusteella voidaan saada selville, toimitaanko kohteessa primaariaineiston ja haastattelun mukaisella tavalla (Hirsjärvi ym. 2009, 212).

Tiedonkeruun kohteina ovat ensisijaisesti ihmiset, joita tukevat ja täydentävät kirjallinen materiaali. Lähtökohtana tutkimukselle ovat tutkittavan aineiston moniulotteinen ja yksityiskohtainen tarkastelu eikä niinkään testata olemassa olevaa teoriaa tai hypoteesia. Tätä kutsutaan induktiiviseksi analyysiksi, jonka tarkoituksena on odottamattomien asioiden paljastaminen. Kvalitatiivisessa tutkimuksessa aineiston hankinnassa käytetään myös laadullisia metodeja, joita tässä opinnäytetyössä ovat dokumenttien analyysit, osallistuva havainnointi ja strukturoidut haastattelut. Tutkimuksen kohdejoukon valitseminen ei ole kvalitatiivisessa tutkimuksessa satunnaista, vaan tarkoituksenmukaista. (Hirsjärvi ym. 2009).

Tämän opinnäytetyön tutkimuskysymysten selvittäminen ovat kvalitatiivisen tutkimukselle ominaista todellisen elämän kuvaamista. Turvallisuuden johtamisesta vastaavat viime kädessä ihmiset, joten on hyvin luonnollista, että ne myös toimivat ensisijaisina tiedonlähteinä tutkimukselle. Turvallisuusdokumenttien tarkastelu ja analysointi laadullisena metodina ovat niin ikään ihmisten aikaan saamia asiakirjoja. Tämän opinnäytetyön haastattelukohderyhmän valinta on erityisessä asemassa. On tärkeätä, että turvallisuusjohtamista tarkastellaan monesta eri näkökulmasta.

Ensisijaisena tiedonkeruumenetelmänä tässä tutkimuksessa käytetään yksikön turvallisuusdokumenttien ja – asiakirjojen havainnointia, joita tarkastelemalla turvallisuusjohtamisen tasoa

pyritään todentamaan. Myös virallisessa KATAKRIn auditointiprosessissa ensimmäiseen vaiheeseen kuuluu dokumenttien tarkastelu. Näin tässäkin tutkimuksessa yhtenä tiedonkeruumenetelmänä käytetään virallisten dokumenttien tarkastelua. Sen tarkoituksena on löytää mahdollisimman kattavasti vastauksia auditointiraportin kysymyksiin. Dokumentteina pyritään käyttämään kaikkia mahdollisia turvallisuusdokumentaatioita, mitä kohdeyksikkö on tuottanut.

Toisena tiedonkeruumenetelmänä käytetään strukturoituja haastatteluja eli lomakehaastatteluja. Haastattelukysymykset muodostuvat Kansallisen turvallisuusauditointikriteeristön osioon hallinnollisesta turvallisuudesta. Hirsjärven ym. (2009, 208) mukaan strukturoitu haastattelu eli lomakehaastattelu tapahtuu sellaista lomaketta apuna käyttäen, missä kysymysten esittämisjärjestys ja muoto on ennalta määrätty. Strukturoitua haastattelua käytetään tässä opinnäytetyössä dokumenttien tarkastelun tukena ja toisena tiedonkeruumenetelmänä.

Haastattelut toteutetaan yksilöhaastatteluina ja niiden avulla pyritään selventämään ja syventämään niitä tietoja, joita on jo saatu selville dokumenttien tarkastelusta. Haastattelun strukturoituna lomakkeena käytetään auditointiraporttipohjaa, minkä kysymykset ovat KATAKRIn hallinnollisen turvallisuuden osa-alueen kysymyssarjasta. Hirsjärven ja Hurmeen (2009, 44–45) mukaan lomakehaastattelu on yksi käytetyimmistä haastattelulajeista. Suurimpana haasteena strukturoiduissa haastatteluissa on muotoilla kysymykset ja haastattelulomake. Lomakkeessa esille tulevat käsitteet ja vaihtoehdot tulevat tässäkin tapauksessa KATAKRIsta. Haastateltavalla ei näin välttämättä ole käsitystä siitä, mitä kullakin auditointikriteeristön kysymyksellä tarkoitetaan.

Kolmantena tiedonkeruumenetelmänä käytetään observointia eli havainnointia, jossa suojaustasojen vaatimusten täyttymistä tarkkaillaan lukemalla, näkemällä ja toimimalla itse kohteessa. Dokumenttien tarkastelun ja haastattelun perusteella saadaan selville kirjoitettu tieto sekä haastateltavien ajatukset auditointikysymyksistä. Ne eivät kuitenkaan kerro, mitä yksikössä todella tapahtuu. Havainnoinnin avulla pystytään saamaan tietoa siitä, pitävätkö dokumenttien ja haastattelujen avulla saatu tieto paikkansa (Hirsjärvi ym. 2009, 212). Havainnointia ei tule siis rajoittaa vain pelkästään asioiden näkemiseen. Havainnointi on tarkkailua, jonka avulla voidaan saada välitöntä ja suoraa tietoa yksikön toiminnasta. Havainnoinnin lajeista tässä tutkimuksessa käytetään osallistuvaa havainnointia (2009, 216-217). Siinä tutkija itse osallistuu kohdeyksikön toimintaan ja on osana havainnoitavan kohteen työyhteisöä.

Ojasalon, Moilasen ja Ritalahden (2009, 42) mukaan havainnointi on suositeltava menetelmä kaikessa kehittämistyössä. Menemällä itse paikan päälle tarkkailemaan todellista toimintaa saa usein realistisemman ja hyödyllisemmän tiedon kuin pelkästään haastatteluilla. Ojasalo ym. (2009, 42) pitävät kenttäpäiväkirjan täyttämistä järjestelmällisenä havainnointien ke-

ruumenetelmänä. Kenttäpäiväkirjaa tulisi täyttää koko kehittämisprosessin ajan, vaikka samaan aikaan käytettäisiin jotain muuta tutkimusmenetelmää.

Tässä opinnäytetyössä täytetään havainnointipäiväkirjaa koko auditointiprosessin ajan. Tarkoituksena on tarkkailla kohteen turvallisuusjohtamisen toimintaa lukemalla, näkemällä ja osallistumalla. Havainnoinnin aikana tulee analysoida jo muilla tavoin esille tulleita suojaustasovaatimusten puutteita käytännön näkökulmasta. Suojaustasoa ei välttämättä saavuteta turvallisuusdokumenttien tai haastatteluista saatujen tietojen perusteella. Havainnoinnin avulla voidaan saada selville, onko tasovaatimusten saavuttamiseen olemassa joitain vaihtoehtoisia tapoja.

Opinnäytetyön kvalitatiivisen tutkimusmenetelmän lajina käytetään hermeneuttista menetelmää. Hermeneutiikka tulee sanana kreikan kielestä ja sillä tarkoitetaan julistamisen, tulkkauksen, selittämisen ja tulkinnan taitoja. Hermeneutiikassa kyse on myös ymmärtämisen taidoista silloin, kun jokin asia ei ole yksiselitteinen (Gadamer 2004, 40). Kivelän ja Sutisen (2009, 73) mukaan hermeneutiikka ymmärretään niin tulkintaopiksi tai -taidoksi kuin tutkimusmenetelmälliseksi lähtökohdaksi. Sitä voidaan luonnehtia taito-oppina ymmärtämiseen tai taitona ymmärtää toisen puhe oikein.

Hermeneuttinen menetelmä tutkimuslajina perustuu Gadamerin (2004, 29-35) mukaan hermeneuttiseen kehään, jossa kokonaisuuden ymmärtäminen perustuu suoraan ennakointiin. Kokonaisuuden osat tulisi siten ymmärtää itsensä määrittäjinä. Aivan niin kuin auditointitapahtumissakin, auditoijan ennakkoluulot kohteesta eivät saa ottaa kuitenkaan valtaa tulosanalyysin lopputulokseen. Ennakkoluuloille tulee antaa oikeutus eli tutkijan tulee tutkia niiden alkuperää ja pätevyyttä. Omia mielipiteitä ei tule siis täysin sivuuttaa, koska se on osa auditoitavan kohteen ymmärtämisen kehittymistä. Tässä tutkimuksessa hermeneuttisella kehän puoli on subjektiivinen, sillä kohdetta kokonaisuutena arvioidaan ensin ennakoivasti, jonka jälkeen sitä yksityiskohtaisesti tutkitaan.

3 Turvallisuusauditoinnin teoria

Tutkimuskysymysten, teoreettisen viitekehyksen ja tutkimusmenetelmien esittelyn lisäksi esitellään myös turvallisuusauditointiin liittyvää teoriaa, jotka ovat osana luomassa tutkimuksen perustaa. Käsitteiden ymmärrystä tarvitaan, jotta itse tutkimusta olisi helpompi arvioida ja lukea (Heinonen ym. 2013, 29-30). Tämän tutkimuksen keskeistä teoriaa ovat Kansallinen turvallisuusauditointikriteeristö KATAKRI, turvallisuusjohtaminen, riskienhallinta ja auditointi. Keskeisten teorioiden lisäksi tutkimuksessa käytetään myös muita turvallisuusjohtamiseen liittyviä termejä, joita kuvataan tässä luvussa myös tarkemmin.

3.1 Kansallinen turvallisuusauditointikriteeristö

Kansallinen turvallisuusauditointikriteeristö KATAKRI syntyi osana Suomen hallituksen sisäisen turvallisuuden ohjelmaa. Sen tarkoituksena oli luoda yhteinen kriteeristö turvallisuusauditointeihin niin viranomaisille kuin yrityksille. Yhteisellä kriteeristöllä on tarkoitus yhtenäistää menettelyjä turvallisuuden hallinnassa sekä parantaa omavalvontaa ja auditointia. KATAKRIn päätavoitteena on viranomaistoimintojen yhdistäminen organisaatioissa toteutettavien turvallisuustason tarkastuksien todentamisessa. Toinen päätavoite on auttaa muita organisaatioita sekä viranomaisia sidosryhmineen omassa sisäisessä turvallisuustyössä. (Puolustusministeriö 2011).

KATAKRI koostuu neljästä eri turvallisuuskokonaisuudesta. Niitä ovat hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus ja tietoturvallisuus. Hallinnollisella turvallisuuden kysymyssarjalla todennetaan turvallisuusjohtamisen tasoa tämän opinnäytetyön auditoitavassa kohteessa, jossa mitataan erityisesti turvallisuusjohtamisjärjestelmän toimivuutta (Puolustusministeriö 2011). KATAKRI perustuu niin sanottuun security-näkökulmaan, joten turvallisuusjohtamisen tarkastelusta on poissuljettu niin sanottuun safety-näkökulmaan rajatut aiheet. Näitä ovat muun muassa palo- ja työturvallisuuden johtaminen.

KATAKRIa hyödynnetään viranomaispuolella erityisesti sellaisissa hankkeissa, joissa ulkopuoliselta yritykseltä vaaditaan yksityiskohtaisten suojausvaatimusten täyttymistä eri turvallisuusluokissa (Ulkoministeriö 2011). Tämän opinnäytetyön ensisijainen tavoite on KATAKRIn avulla todentaa kohteen turvallisuusjohtamisen taso. Tarkoituksena ei ole suorittaa varsinaista, KATAKRIn mukaista turvallisuusauditointia. KATAKRIn suojaustasovaatimusten avulla pyritään tehdä sellainen esiauditointi, joka mahdollisesti voisi valmentaa kohdetta varsinaiselle auditoinnille. Näin varsinaisen tavoitteen lisäksi yritetään saada selville, miten KATAKRI soveltuu sellaiseen viranomaisympäristöön, missä auditointi tai standardinmukaisuus on ylipäätään vieras käsite.

KATAKRIn mukaisissa turvallisuusauditoinneissa korostuu auditoijan ja auditoitavan kohteen vuorovaikutus. Ennen varsinaisia auditointihaastatteluja, auditoijan tulee etsiä vastauksia kysymyksiinsä dokumenteista ja asiakirjoista. Vakavien puutteiden ilmetessä jo dokumentaatiovaiheessa, niistä tulee tiedottaa välittömästi kohteelle (Puolustusministeriö 2011). Reimanin ja Oedewaldin (2008, 344) mukaan pelkkä dokumenttien ja asiakirjojen tarkastelu ei kuitenkaan paljasta organisaation havaitsemattomia vaaroja. Dokumenteille ei pysty myöskään osoittamaan, miten organisaatio käytännössä toteuttaa turvallisuuden hallintaa.

Jotta käytännön arviointia muodostuisi asiakirjojen rinnalle, dokumentaatiovaiheen jälkeen auditoija tekee suunnitelman tarkastettavista kohteista. Auditointitapahtuman tulokset kirja-

taan ylös, jonka perusteella nähdään vaatimusten täyttymiset ja poikkeamat. Mikäli jotain KATAKRIn asettamaa suojaustasoa ei pystytä täyttämään, auditoitavan kohteen tulee osoittaa tälle jokin korvaava turvallisuusmenettely. Auditoinnista annetaan kohteelle suullinen palaute välittömästi sen päätyttyä sekä myöhemmin kirjallinen raportti. Auditointeja toistetaan niin pitkään kunnes kohde täyttää sille asetetun suojaustason vaatimukset. (Puolustusministeriö 2011)

Tämän opinnäytetyön auditoitavan kohteen kysymykset ovat sen hallinnollisen turvallisuuden korotetun tason suojausvaatimuksista. Organisaatio, jonka suojausvaatimukset ovat korotetun tason mukaisia, tiedostaa turvallisuusasioiden merkityksen koko organisaatiolle. Sellaisessa organisaatiossa on edistytty turvallisuustoimenpiteissä, vaikka välttämättä turvallisuusnäkökulma ei ole osana ydintoimintaa (Paasonen, Huumonen ja Paasonen 2012, 92). Korotetun tason vaatimuksista on kuitenkin hyvä kohteen lähteä liikkeelle. Niissä esitetyt kysymykset antavat hyvän tilanneanalyysin vallitsevasta turvallisuuden tasosta.

Korotettua taso alempi, Perustason organisaatio tarkastelee yksittäisesti turvallisuuden eri osa-alueita. Tällaisessa organisaatiossa turvallisuusjohtaminen ei ole systemaattista. Perustason organisaatiossa yleensä ei ole budjetoitu erikseen resursseja turvallisuuden kehittämiseen ja turvallisuusvaatimusten tavoitteina ovatkin vain sidosryhmien vaatimusten täyttäminen. Korotettua tasoa paremmassa, Korkean tason organisaatiossa turvallisuustoiminta huomioidaan kaikessa toiminnassa. Tämän suojaustason täyttävässä organisaatiossa on omaksuttu turvallisuuden jatkuvan kehittämisen merkitys (Paasonen ym. 2012, 91-93).

3.2 Turvallisuusjohtaminen

Turvallisuusjohtamisella pyritään hallitsemaan kaikkia organisaation turvallisuusasioita. Organisaatioturvallisuus on tae organisaation toimintaedellytyksille sekä tuotannon ja toiminnan häiriöttömyydelle. Sillä myös suojataan organisaation henkilöstöä, omaisuutta, tietoa ja ympäristöä vahingoilta, onnettomuuksilta ja rikolliselta toiminnalta. Turvallisuusjohtaminen on ennakoivaa toimintaa, jolla luodaan toimintavalmiuksia (Kerko 2001, 21). Paasosen ym. (2012, 79-80) mukaan turvallisuusjohtaminen kuuluu organisaation normaaliin johtamisprosessiin ja sillä pyritään hallitsemaan turvallisuutta kokonaisvaltaisesti. Turvallisuustoimintaan liittyvien sääntelyvaatimusten täyttäminen ja omaehtoinen turvallisuustyö kuuluvat pääasiallisiin tehtäviin turvallisuusjohtamisessa. Organisaatio voi vaatimusten lisäksi suunnitella myös omia toimenpiteitä turvallisuuden edistämiseksi.

Turvallisuusjohtamisen on oltava organisaation jokapäiväistä toimintaa ja jokaisen työntekijän tulisi olla sitoutunut sen menestykselliseen toteuttamiseen. Parhaat edellytykset siihen sitoutumiseen luovat henkilöstön koulutus ja tiedotus sekä osallistuminen suunnitteluun ja

päätöksentekoon. Näin työntekijät näkevät itse turvallisuusjohtamisen isompana kokonaisuutena eikä sen toteuttamista pidetä vain jonkun erillisen asiantuntijan tehtävänä. Organisaationjohto vastaa viime kädessä turvallisuustoiminnan organisoinnista. Siihen kuuluu strateginen työskentely, käytännön turvallisuustoiminnot, työpaikkojen omavalvonta ja riskienarviointitoiminta sekä määrittely muista vastuista ja velvoitteista. (Kerko 2001, 40).

Turvallisuusjohtaminen on kokonaisvaltaista turvallisuuden johtamista. Ilman turvallisuusorientoitunutta suhtautumista asiaan, sitä voi olla vaikea hahmottaa tai välttämättä siihen ei osaa kiinnittää tarpeeksi huomiota. Turvallisuusjohtamisen käsittämisessä ja hahmottamisessa avainasemassa on se konteksti, minkä yhteydessä asiasta puhutaan. Eri ammattialoilla turvallisuus ilmiönä saatetaan nähdä monin eri tavoin. Esimerkiksi rakennustyömaiden kaltaisilla työpaikoilla turvallisuusjohtaminen saatetaan nähdä vain työturvallisuuden johtamisena, koska niissä yleisimmin työskennellään työkoneiden, melun, lian ja fyysisen rasituksen parissa. Toisaalta paljon tietotekniikkaa tai tietojen käsittelyä sisältävissä organisaatioissa turvallisuusjohtaminen saatetaan kokea tietoturvallisuusjohtamisena tai jätehuoltolaitoksissa se ymmärretään ympäristöturvallisuusjohtamisena jne. Edellä mainitut näkökulmat ovat täysin ymmärrettävissä organisaation työntekijätasolla. Organisaation johdon tulee käsittää asia paljon laajemmin: heidän vastuullaan on organisaation kokonaisturvallisuus ja niiden tulee osata hallita sitä kokonaisvaltaisesti jokaisella eri osa-alueella.

Suomessa turvallisuusjohtamisen ja riskienhallinnan ensimmäiset vaikutteet saatiin ulkomailta 1980-luvulla, kun suomalaiset organisaatiot alkoivat kansainvälistyä. Turvallisuusjohtamisen käsite ei juurtunut heti suomalaiseen kieleen, mutta riskienhallinta käsitteenä omaksuttiin käyttöön erityisesti vakuutusyhtiöissä. Turvallisuusjohtaminen oli ollut siis joissakin maissa pidemmällä kuin Suomessa, mutta vähitellen eurooppalaisten direktiivien pohjalta alettiin rakentaa myös Suomen turvallisuuslainsäädäntöä. Nykytilanne on kehittynyt aikojen saatossa pidemmälle. Kerko (2001, 12-17) toteaa, että suomalaisissa organisaatioissa tunnetaan tänä päivänä yhä enemmän mielenkiintoa turvallisuusasioita kohtaan. On tiedostettu, että onnettomuudet, tapaturmat ja sairaslomat vaikuttavat yrityksen kannattavuuteen sekä maineeseen. Turvallisuuden takaamista yrityksissä säädetään lailla, mutta sen liiketoiminnallista merkittävyyttä ei vielä täysin ymmärretä.

Riskienhallinta-ajattelun tai riskiperusteisen turvallisuusjohtamisen myöhäinen liittyminen suomalaiseen johtamiskäytäntöön on saattanut jarruttaa myös organisaatioiden turvallisuuskulttuurin muodostumiseen. Vastakohta tällaiselle ajattelulle turvallisuuspoikkeamiin puuttuminen vasta silloin, kun jotain ikävää on tapahtunut. Poikkeamiin puuttuminen ei siis varauduta, mikä on yksi turvallisuusjohtamisen lähtökohdista. Riskien arviointi, riskien analysointi ja riskien hallinta ei ole siis tarkoituksenmukaisessa toiminnassaan. Riskiperusteisen turvallisuusjohtamisen tuominen ja markkinoiminen organisaatioon tulisi kuitenkin tuottaa

sille lisäarvoa, jotta turvallisuutta ei nähtäisi pakollisena, lainsäädännöllisenä haittana. Turvallisuuden johtaminen tulisi liittää luonnollisena osana muuta johtamista ja sen taloudellisuutta nähdä kokonaisvaltaisesti lisäarvoa tuottavana, eikä niinkään lyhytkatseisena menoeränä.

Turvallisuusjohtamisen yksi perusta on strateginen johtaminen. Sen tarkoitus on suunnata organisaation prosessit kohti johdon visiota halutusta tilasta sekä tuottaa sidosryhmille lisäarvoa. Strategialla tarkoitetaan organisaation tavoiteltua toiminnan ihannetilaa, jossa tulee ottaa huomioon sekä nykyiset että tulevaisuuden tarpeet. Olennainen osa strategista johtamista on strateginen suunnittelu, joka pohjautuu organisaation visioille ja arvoille. Strategisessa suunnittelussa tehdään pitkän tähtäimen suunnitelmia, jotta saavutettaisiin tietty päämäärä. Strategiaan kuuluu olennaisena osana parhaiden mahdollisten käytäntöjen valitseminen, jotta organisaation tavoitetilaan tai visioon päästäisiin. (Paasonen ym. 2012, 89-93)

Organisaation turvallisuusjohtamisen perusteita viitoitetaan ja linjataan strategisella johtamisella. Nämä linjaukset toimivat pohjana operatiiviselle turvallisuusjohtamiselle ja samalla kaikkeen turvallisuustoimintaan. Selkeän strategisen turvallisuusjohtamisen puuttuminen tuo ongelmia operatiiviseen johtamiseen. Ilman strategista perustaa työntekijöiden lähimmillä esimiehillä ei välttämättä ole käytössään tarvittavia operatiivisia turvallisuusjohtamisen työkaluja alaistensa johtamiseen. Ylimmän johdon tulee ottaa vastuu turvallisuusjohtamisesta ja asettaa sille strategiset päämäärät, jotta epävarmuutta tai päätöksentekokyvyttömyyttä ei turvallisuustoiminnan käytänteistä puuttuisi.

Toisin kuin strategisessa turvallisuusjohtamisessa, operatiivisessa turvallisuusjohtamisessa keskitytään lyhyisiin ajanjaksoihin ja pieniin kokonaisuuksiin. Se on osa päivittäistä johtamista, jossa esimies valvoo työntekijöitään niiden tavoitteellisissa onnistumisissa. Operatiivisessa johtamisessa esimiehen tehtäviin kuuluu myös tukea työntekijöitään ja analysoida riskejä. (Paasonen ym. 2012, 89)

Käytännössä operatiivinen johtaminen on juuri sitä työntekijälle näkyvintä johtamista. Oman lähiesimiehen toiminta on todella ratkaisevaa yksittäisen työntekijän suhtautumiseen turvallisuusasioihin. Operatiivisen turvallisuusjohtajan tulee omassa toiminnassaan noudattaa organisaation strategisia päämääriä ja suhteuttaa ne omaan johtamiseen. Tässä on otettava huomioon mahdollisen strategisen turvallisuusjohtamisen puuttuminen, joka aiheuttaisi ongelmia operatiivisessa johtamisessa. Operatiivisella tasolla tulee olla myös vuorovaikutteinen strategiseen tasoon. Lähiesimiehen suorittamat riskien arvioinnit tai muu turvallisuustoiminnan kehittäminen tulee ottaa huomioon ylimmässä johdossa ja strategisessa suunnittelussa.

Turvallisuusjohtamisen tulee perustua valittuihin ja päätettyihin toimintaperiaatteisiin ja politiikkoihin. Näin muodostetaan organisaatiolle turvallisuuspolitiikka. Se on strateginen ohjelma, jolla halutaan mm. turvallisuus tärkeäksi osaksi liiketoimintaa, turvallisuushallintajärjestelmän aikaansaaminen, riittävät resurssit, menettelytapoja, henkilöstön sitoutuminen, koulutuksen varmistaminen, katselmusten suorittaminen ja riskiperiaatteen huomioiminen sekä vastuiden, velvoitteiden ja valtuuksien määritys. Turvallisuuspolitiikassa tulisi ilmetä yrityksen turvallisuuskulttuuria ohjaavat arvot ja se tulisi lausua tiivistetyllä ja ymmärrettävällä tavalla. (Kerko 2001, 44-46)

Turvallisuuspolitiikkaa voisi Kerkon (2001, 46-47) kuvauksen mukaisesti pitää yhtenä organisaation turvallisuustoiminnan perusteena tai mainoslauseena. Turvallisuuspolitiikan perusteella voidaan tehdä nopeita ensivaikutelmia siitä, miten organisaatiossa ylipäätään suhtaudutaan turvallisuuteen. Turvallisuuspolitiikan tärkeyttä ei voine korostaa liikaa ainakaan ulkopuolisen näkökulmasta, mutta toisaalta se auttaa myös organisaatiota sisäisesti hyvän turvallisuuskulttuurin ylläpitämisessä. Turvallisuuspolitiikan kattavuudesta tai olemassaolosta ylipäätään pystyy tekemään johtopäätöksiä, jotka voivat olla merkittäviä organisaation kannalta. Esimerkiksi potentiaaliset työntekijät tai yhteistyökumppanit saattavat nähdä siinä johdon antaman tuen ja vastuun omalle turvallisuustyölleen.

Turvallisuuskulttuuri on osa organisaatiokulttuuria. Siinä on kyse merkityksistä ja käytännöistä, joilla varaudutaan riskeihin ja epätoivottuihin tilanteisiin sekä turvallisuustasosta, jonka organisaation johto hyväksyy. Turvallisuuskulttuurilla on vahva sidos turvallisuusjohtamiseen, koska se on organisaation tapa toimia turvallisuusasioissa. Turvallisuuskulttuuri on kyky ja tahto ymmärtää turvallisuutta. Siinä korostuu voimakkaasti myös henkilöjohtamisen merkitys, koska kulttuurin kehittämisessä on olennaista henkilöstön motivaatio ja läsnäolo. Henkilöstö saadaan mukaan parhaiten, jos turvallisuutta lähestytään työviihtyvyyden ja inhimillisten tarpeiden näkökulmasta. Turvallisuusjohtamisen olennainen osa on turvallisuuskulttuurin ymmärtäminen. Turvallisuuskulttuurin johtamiseen kuuluvat selkeät toimintatavat ja ohjeet, monipuolinen viestintä sekä kattava kommunikointi turvallisuustasosta, riskeistä ja hyväksyttävistä toimintatavoista. Johdon ja henkilöstön tulee todella sitoutua hyvän turvallisuuskulttuurin luomiseen, jotta sen edellytykset täyttyisivät. (Paasonen ym., 2012, 96-99)

Organisaation ylimmän johdon tulee sitoutua hyvän turvallisuuskulttuurin luomiseen osana turvallisuusjohtamista. Ylin johto omalla esimerkillään ja johtamisellaan osoittaa turvallisuudelle merkityksen. Jos turvallisuuspolitiikka oli sitoutuneisuuden esille nostamista ja imagon esille tuomista, turvallisuuskulttuurin luomisella pureudutaan asiassa paljon syvemmälle. Politiikka ei yksistään riitä toteuttamaan turvallisuutta organisaation sisällä, vaan sitoutuminen tulee osoittaa myös käytännössä. Turvallisuuskulttuuriin panostetaan niin taloudellisilla resursseilla kuin uskottavalla turvallisuuden hallintajärjestelmällä. Sen jalkauttaminen käytän-

töön antaa vahvan tukirakenteen turvallisuustoiminnan julkituonnille: hyvän turvallisuuskulttuurin ansiosta organisaatio pystyy rakentamaan uskottavan turvallisuuspolitiikan.

Kerkon (2001, 20–21) mukaan laajaan turvallisuustoimintaan kuuluu turvallisuus (Safety), terveys (Health), ympäristö (Environment) ja laatu (Quality). Kokonaisturvallisuuteen kuuluu kaikki kymmenen organisaatioturvallisuuden osa-aluetta, joita ovat rikosturvallisuus, tuotannon ja toiminnan turvallisuus, työturvallisuus, ympäristöturvallisuus, pelastustoiminta, valmiussuunnittelu, tietoturvallisuus, henkilöturvallisuus, toimitilaturvallisuus ja ulkomaantoimintojen turvallisuus. Jotta organisaatio pystyisi hallitsemaan kaikkia näitä turvallisuuden eri osa-alueita, olisi niille kuitenkin luotava yksi turvallisuuden hallintajärjestelmä. Organisaatiossa asiantuntemus eri turvallisuuden osa-alueilla monesti hajautuvat useille toimijoille. Näin yhdelläkään toimijalla ei ole mahdollisuutta tunnistaa ja ratkaista toisiinsa kytkeytyviä ongelmia. Turvallisuuden kehittämiseen on luotava siis ennakkoluuloton toimijoiden välinen yhteistyö, turvallisuusjohtamisjärjestelmä (Paasonen ym. 2012, 93-96).

Turvallisuusjohtaminen perustuu laatujohtamisen malliin. Toistaiseksi turvallisuusjohtamisjärjestelmät eivät ole täysin vakiintuneet ja niiden sisällöt saattavat vaihdella useisiin turvallisuuden eri osa-alueisiin. Turvallisuusjohtamisjärjestelmien elementteihin kuuluvat organisaatiorakenne, resurssit ja vastuualueet. Yhden johtamisjärjestelmän tarkoitus on tuottaa suurempaa synergiaetua kuin useat erilliset järjestelmät, joita käytetään yhtäaikaisesti (Paasonen ym. 2012, 93-96). Turvallisuusjohtamisjärjestelmä auttaa organisaatiota toimimaan lainsäädännön mukaan ja täyttämään EU-direktiivien mukaisia turvallisuusnormeja. Se vaikuttaa myös yhteistyösopimusten ja yhteistyöverkostojen syntymiseen (Kerko 2001, 32).

Turvallisuusjohtamisjärjestelmät ovat järjestelmällisiä, mutta myös taloudellisia ja kustannustehokkaita. Avainasemassa siinä on tärkeä synergiaetu. Johtamisjärjestelmän kaltaisella työkalulla pystytään liittämään samaan järjestelmään kaikki turvallisuuteen liittyvät laatujärjestelmät. Tämä sopii yhteen hyvin myös riskienhallinta-ajattelun kanssa, jossa pyritään hallitsemaan kaikki riskejä kokonaisvaltaisesti. Hallintajärjestelmän avulla saadaan yhteen myös eri turvallisuuden aloista vastaavat, joka lisäisi sidosryhmäyhteistä sekä toisi dynaamisuutta kokonaisvaltaiseen turvallisuusjohtamiseen.

Turvallisuus käsitetään hyvin usein organisaatioissa ja varsinkin sen johdossa tukitoiminnaksi, jonka turvallisuusinvestoinnit tuovat vain kustannuksia. Turvallisuustoimintaan liittyville investoinneille on kuitenkin vaikeaa määrittää rahallista arvoa. Todellinen hyötykin voi olla vaikeasti testattavissa ja osoitettavissa esimerkiksi turvallisuustekniikan osalta. Investoimalla turvallisuuteen tuleekin katsoa asioita laajoista näkökulmista, eikä tuijottaa vain siitä aiheutuvia kustannuksia. (Paasonen ym. 2012, 85-89)

Turvallisuuden järjestelmällisellä hallinnalla pyritään tuomaan lisäarvoa organisaatiolle. Lisäarvon löytäminen ja sen osoittaminen organisaation toimintaan saattaa olla kuitenkin haasteellista. Turvallisuuteen liittyviä kustannuksia ei tule esittää sellaisenaan. Organisaation johdon tulee ottaa huomioon asian laajempi näkökulma: miten lisäarvo organisaatiolle tehdään? Esimerkiksi jonkin tietyn turvallisuussertifikaatin hankkiminen kasvattaa lisäarvoa tuntuvasti. Sertifikaatin hankkimisen taustalla ovatkin tietyt standardit, jotka organisaation tulisi täyttää ja niiden avulla saadaan kehitettyä kokonaisturvallisuutta.

3.3 Riskienhallinta

Riskienhallinnalla muodostetaan myös yksi perusta turvallisuusjohtamiselle. Siinä on kyse riskien tunnistamisesta ja riskien todennäköisyyksien sekä toteutumisen arvioinnissa. Riskienhallinta noudattaa niin sanottua kehämallia, jossa riskejä arvioidaan jatkuvasti uudelleen toimintaympäristön muutosten keskellä. Riskejä hallitaan systemaattisella toiminnalla, jolla pyritään varmistamaan häiriötön toiminta. Riskeihin varaudutaan niiden estämisellä, vähentämisellä, siirtämisellä tai jatkuvuussuunnittelulla. Riskienhallinta on osa jokapäiväistä toimintaa, johon on olennaista määritellä tarkoitus, tavoitteet, roolit ja vastuut. Organisaation riskit kohdistuvat sen maineeseen, henkilöstöön, tietoon, ympäristöön ja omaisuuteen. Organisaatio voi ottaa käyttöönsä riskienhallintamallin, jolla pyritään varmistamaan toimintojen tehokkuus ja tarkoituksenmukaisuus, taloudellisen tiedon ja raportoinnin luotettavuus sekä sääntelyn noudattaminen. (Paasonen ym. 2012, 80-85)

Riskienhallintaan on olemassa ISO 31000 – standardi, jonka avulla organisaatiot pystyvät kehittämään riskienhallintansa vaatimusten mukaiselle tasolle. Sen avulla pystytään luomaan luotettava tapa tunnistaa, hallita ja ottaa tietoisia riskejä. Standardin kautta organisaatio kykenee tunnistamaan tarpeet riskien tunnistamiseen ja käsittelyyn koko organisaatiossa. Se edesauttaa raportointia ja hyvän hallintotavan toteuttamista sekä kehittää ennakoivaa johtamista. Sertifioinnin perustaksi ISO 31000 -standardia ei ole kuitenkaan tarkoitettu. (Suomen Standardisoimisliitto 2013)

Riskienhallinta alkaa riskien tunnistamisella, koska tunnistamattomia riskejä ei voi hallita. Riskien tunnistaminen tarkoittaa sitä, että erilaisia menetelmiä hyödyntämällä havaitaan ennakolta riski- ja vaaratilanteita. Tunnistusmenetelmien tulee olla monipuolisia ja niiden perusteella tulee pystyä arvioimaan riskin mahdollisuus ja todennäköiset seuraukset. Riskien tunnistamisella voidaan saada näkyviin myös piilossa olevia riskejä, mitkä eivät muuten olisi havaittavissa (Flink, Reiman & Hiltunen 2007, 131).

Riskien analysoinnin tavoitteena on tunnistaa kohteen riskit sekä arvioida niiden todennäköisyydet ja odotettavissa olevat vahingot. Riskianalyysia voidaan tarkastella teknisesti, jolloin

tunnistetaan ja arvioidaan riskiä, jonka tuottaa jokin tekninen järjestelmä. Riskikohteet käydään systemaattisesti läpi, jonka avulla pyritään selvittämään vahingon todennäköisyydet ja seuraukset. Riskianalyysi voi olla myös laajempi käsite, jolloin sillä tarkoitetaan kokonaisuutta, johon kuuluu riskin määrittäminen, arviointi, kokeminen ja hallinta. Käytännössä kyse on jo riskienhallintaprosessista. (Flink ym. 2007, 136).

Riskianalyysimenetelmiä on erilaisia. Jokaiseen riskiin tarvitaan juuri siihen sopiva menetelmä, jolloin on otettava huomioon organisaation eri toiminnot ja niiden laajuus. Riskien analysointi on yhteistyötä, jossa organisaation eri toimijat tekevät analysointityötä yhdessä alusta alkaen. Käytännössä jokaisesta eri henkilökuntaryhmästä tulisi olla osallistujia analyysiryhmässä, jotta riskitietoisuus eri aloilta leviäisi kaikkien keskuuteen. Riskianalyysin perimmäisenä tarkoituksena on saada riskit tärkeysjärjestykseen, mutta tärkein vaihe on sopia tunnistettujen ja tärkeysjärjestyksessä olevien riskien hallintatoimenpiteistä. (Flink ym. 2007, 137-138).

Riskien tunnistusten ja tärkeysjärjestykseen laittamisen jälkeen voidaan tehdä päätöksiä niiden hallintatoimenpiteistä. Päätöksissä tulee ottaa huomioon hallintakeinojen toteutusmahdollisuudet sekä kustannukset. Riskien hallintatoimenpiteet ovat säätelyä, jonka avulla organisaatiota estetään ottamasta vahingollisia riskejä toiminnassaan. Riskejä voidaan siirtää, jolloin seurausten vastuu siirretään toiselle taholle joko kokonaan tai osittain. Riskin poistamisella tarkoitetaan sen konkreettista poistamista. Tässä tapauksessa riski pyritään jollain tavoin kokonaan pyyhkiä pois organisaation prosesseista. Riskin pitämisellä taas tullaan siihen tulokseen, että organisaation on kannattavampaa pitää riski kuin poistaa se. Tässä tapauksessa riskin sisältävä prosessi vain hyväksytään. Riskiä voidaan myös pienentää, jolloin puututaan riskiä aiheuttavaan asiaan siten, että siitä pienenevät todennäköisyys ja seuraukset. (Flink ym. 2007, 146-148)

Riskienhallinnan omaksuminen turvallisuusjohtamiseen vie turvallisuuden hallinnan organisaatiossa jo hyvin pitkälle. Tätä voidaan kutsua riskiperusteiseksi turvallisuusjohtamiseksi, missä järjestelmällinen ja kokonaisvaltainen riskienhallinta toimii turvallisuusjohtamisen työvälineenä. Organisaation vaillinainen osaaminen riskienhallintaan liittyvistä asioista tai riskienhallintamallin puuttuminen kokonaan muuttaa olennaisesti koko turvallisuusjohtamisen luonnetta. Ilman riskien tunnistamista niihin ei pystytä varautumaan eli turvallisuutta ei pyritä hallitsemaan ennakoivasti.

Riskien tunnistaminen pelkästään tapahtuneiden vaaratilanteiden tai onnettomuuksien avulla haavoittaa organisaation kokonaisturvallisuutta merkittävästi. Kaikkia riskejä voidaan pyrkiä hallitsemaan, mutta kaikista riskeistä ei voi luopua. Täysin riskitöntä organisaatiota ei pysty luomaan. Riskien hallitsemisen lähtökohtana ei voi olla nollatoleranssi uhkien ja vaarojen suh-

teen, vaan tärkeintä on riskien tunnistaminen. Tunnistamattomat riskit luovat yhden isoimmista uhkista organisaatioille. Tunnistettujen riskien puuttuminen saattavat olla kohtalokkaita organisaation toiminnalle ja pahimmassa tapauksessa riskin toteutuminen voi lamauttaa koko toiminnan. Täytyy kuitenkin muistaa, että tunnistetuistakin riskeistä osa tulee hyväksyä sellaisenaan, mikäli muuta toimivaa tai järkevää hallintakeinoa ei pystytä sille järjestämään.

3.4 Auditointi

Auditoinnilla tarkoitetaan organisaatioon kohdistuvaa virallista tarkastusta, joka kohdistuu johonkin tiettyyn prosessiin tai järjestelmään. Auditoinnin suorittaja on pääsääntöisesti organisaatiosta riippumaton taho. Auditointia voidaan kutsua myös järjestelmälliseksi arvioinniksi tai katselmukseksi (Carter 2004, 5). Auditoinnit voidaan luokitella kolmeen erilaiseen arviointitapahtumaan. Näitä ovat sisäinen ja ulkoinen auditointi sekä vertaisauditointi. Auditointien tarkoituksena on hyvin yleisesti pidetty sitä, organisaatio voisi saavuttaa sillä tietyn laatusertifikaatin, jolla pystyisi muille osoittamaan järjestelmänsä toimivuuden. Sertifikaatin saaminen on tällä tavoin vain välineellistä - todellisen hyödyn auditoinnista saa silloin, kun organisaatio ottaa sen mahdollisuutena oppia heikkouksistaan ja vahvuuksistaan. (Reiman & Oedewald 2008, 344).

Johtamisjärjestelmän auditointiin on olemassa myös kansainvälinen standardi SFS-EN ISO 19011. Siinä on ohjeita auditoinnin periaatteisiin, auditointiohjelman hallintaan ja johtamisjärjestelmän auditointien suorittamiseen sekä ohjeita auditointiprosessiin osallistuvien henkilöiden pätevyyden arviointiin. Kyseistä standardia voi soveltaa kaikkiin sisäisiä ja ulkoisia auditointeja toteuttaviin ja suorittaviin organisaatioihin. (Suomen Standardisoimisliitto 2013)

Organisaatioissa voidaan käyttää myös sisäistä auditoijaa tai sisäistä auditointiryhmää. Sisäistä auditointia voidaan Carterin (2004, 25) mukaan pitää parhaana keinona ylläpitää organisaation hallintajärjestelmää. Sisäistä auditointia ei tule sekoittaa sisäiseen tarkastukseen. Simolan (2005, 88) mukaan sisäisen auditoinnin tulee muodostaa kokonaiskuva koko organisaation turvallisuuden tilasta ja niistä saadut havainnot tulee tavoitteellisesti jalkauttaa turvallisuustyöhön. Simola korostaa, että sisäinen turvallisuusauditointi tulee painottua tunnistamaan turvallisuusjohtamisen heikkouksia. Toisaalta, mikäli huomio kiinnittyy liikaa ohjeiden ja vaatimusten puutteisiin tai niiden noudattamisen epäkohtiin, saattaa se jarruttaa itse turvallisuusjohtamisen kehittämistä. Simola katsoo, että sisäinen auditointi voisi käytännössä olla vuosittain tapahtuvaa riskiarviointia tai muita turvallisuuden tasoon liittyviä erityisselvityksiä.

Ulkoinen auditointi on sisäistä auditointia laajempi käsite. Siinä organisaatiosta riippumaton, ulkopuolinen taho tekee paljon laajemman selvityksen organisaation turvallisuuskulttuurista, teknisestä turvallisuudesta, turvallisuusmenettelytavoista tai turvallisuusjohtamisjärjestel-

mästä (Simola 2005, 98). Vertaisauditoinnissa auditointi tehdään niin, että kaksi eri organisaatiota suorittaa auditoinnit toisilleen. Organisaatioiden tulee olla riittävän samankaltaisia, jotta vertaisarvioinnin idea toteutuisi parhaimmalla mahdollisella tavalla. (Reiman & Oedewald 2008, 343)

Vaikka auditointeja ymmärretään tehtävän laajemmin eri laatujärjestelmien sertifioinnin yhteydessä, myös turvallisuusjärjestelmiä arvioidaan samoilla menetelmillä. Turvallisuusauditoinneilla yleensä arvioidaan vahvuuksia ja heikkouksia organisaation turvallisuusjohtamisjärjestelmässä. Sillä pyritään myös tunnistamaan organisaation kohdistuvia vaaroja sekä tuottamaan tietoa turvallisuuden kehittymisestä. (Reiman & Oedewald 2008, 344)

3.5 Muuta teoriaa

KATAKRIn turvallisuusjohtamista tarkastellaan niin sanotusta *security-näkökulmasta*. Koska turvallisuudelle on olemassa suomen kielessä vain yksi sana, organisaatioturvallisuuden karkealle kahtiajaolle on lainattu englanninkielisiä termejä safety ja security. Security-näkökulma käsittää rikosturvallisuuden, kiinteistö- ja toimitilaturvallisuuden, henkilöturvallisuuden ja tietoturvallisuuden osa-alueet. *Safety-näkökulma* taas käsittää pelastustoimintaan, työsuojeluun ja ympäristönsuojeluun liittyvät osa-alueet. Näkökulmien jaottelu ei ole kovinkaan yksiselitteistä ja ne nivoutuvatkin monesti yhteen. (Hallituksen esitys Eduskunnalle laiksi yksityisistä turvallisuuspalveluista sekä eräiksi siihen liittyviksi laeiksi 2001)

Tietoturvallisuus on yksi organisaatioturvallisuuden osa-alue, jolla tarkoitetaan Valtionhallinnon tietoturvallisuuden johtoryhmän eli VAHTI:n mukaan ”tietojen ja palvelujen, järjestelmien ja tietoliikenteen suojaamista ja varmistamista niihin kohdistuvien riskien hallitsemiseksi sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä”. Sen tavoitteena on turvata tietojen luottamuksellisuus, eheys ja käytettävyys. Uhkia ja vahinkoja tietoturvallisuudelle luovat laitteisto- ja ohjelmistoviat, luonnontapahtumat sekä tahalliset, tuottamukselliset tai tapaturmaiset teot. (Valtiovarainministeriö 2007, 13)

Fyysisen turvallisuus on myös yksi organisaatioturvallisuuden osa-alueista. Sillä tarkoitetaan organisaation häiriöttömän toiminnan turvaamista kaikissa olosuhteissa ottaen huomioon riskit ja organisaation erityistarpeet. Fyysiseen turvallisuuteen kuuluu muun muassa kulunvalvonta, kameravalvonta, muu tekninen valvonta ja vartiointi sekä palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunta. (Valtiovarainministeriö 2007, 59)

Henkilöstöturvallisuus on tietoturvallisuuden ja fyysisen turvallisuuden lisäksi organisaatioturvallisuuden osa-alue ja osa security-näkökulmaa. Henkilöstöturvallisuus on henkilöstöstä johtuvaa riskien hallintaa. Sen perustan muodostaa sellainen henkilöstö, joiden toimenkuvissa

on kuvattu selkeästi tietoturvavastuut ja – tehtävät. Keskeisiä asioita henkilöstöturvallisuudessa ovat työhönotto, toimenkuvien olennaiset muutokset ja palvelussuhteen loppumiseen liittyvät prosessit. Olennaista on myös vaarallisten työyhdistelmien tunnistaminen ja poistaminen. (Valtiovarainministeriö 2007, 57)

4 Kohteen auditointi ja tulosanalyysi

Arvioinnin kohteena oleva viranomaisyksikkö auditoitiin 01.10. – 31.10.2013 välisenä aikana. Arvioinnissa käytettiin ensimmäisenä tiedonkeruumenetelmänä turvallisuusdokumenttien tarkasteluja. Dokumentteina toimivat organisaatiotason turvallisuusstrategia ja vaativien tilanteiden ohje sekä yksikön turvallisuus, valmius- ja pelastussuunnitelma. Toisena tiedonkeruumenetelmänä käytettiin auditointihaastatteluja, joiden pohjana toimi strukturoitu haastattelulomake KATAKRIn hallinnollisen turvallisuuden kysymyssarjasta. Haastatteluja tehtiin yksikön neljälle eri työntekijälle, joita olivat turvallisuudesta vastaava esimies, uusi työntekijä, turvallisuuskouluttaja ja apulaisjohtaja. Apulaisjohtajalle, joka toimi ylimmän johdon edustajana, tehtiin kaksi erillistä haastattelua. Viimeisimpänä tiedonkeruumenetelmänä käytettiin käytännön osallistuvaa havainnointia, jota suoritettiin jatkuvasti auditoinnin aikana.

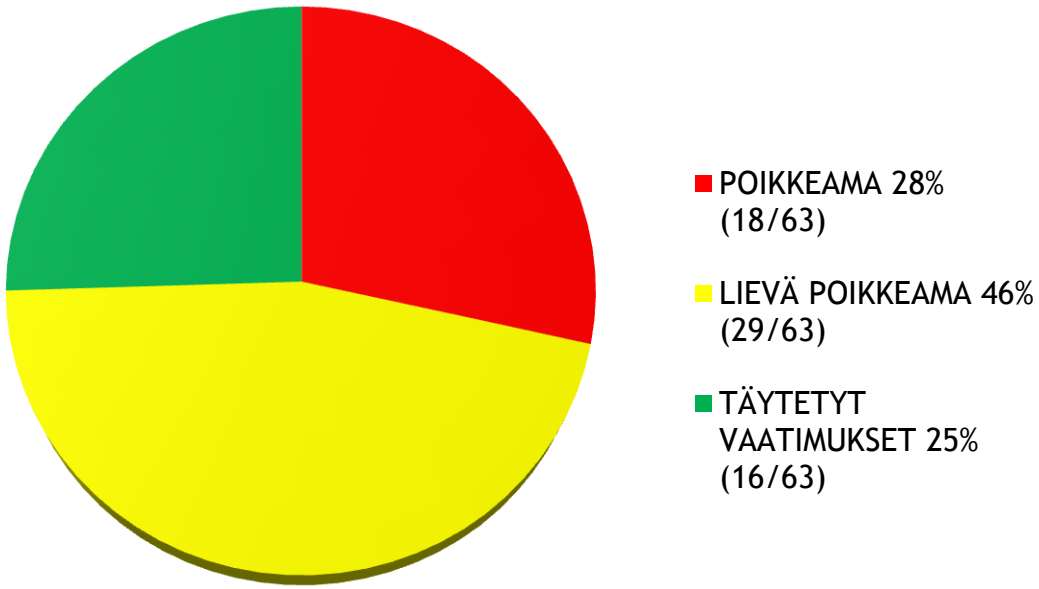
Turvallisuusauditoinnin osa-alueet, kysymykset, suojaustasovaatimukset, havainnot ja poikkeaman tunnistaminen esitetään varsinaisessa auditointiraportissa, joka on opinnäytetyön liitteenä (Liite 1). Suojaustasovaatimuksena käytetään KATAKRIn hallinnollisen turvallisuuden suojaustasovaatimusta korotettu taso III:sta. Korotetun tason suojausvaatimukseen päädyttiin yksikön turvallisuuskriittisen luonteen vuoksi. Tämänkaltaisessa organisaatiossa turvallisuusjohtamiselta tulisi lähtökohtaisesti vaatia enemmän kuin KATAKRIn perustason suojausvaatimuksia.

Hallinnollisen turvallisuuden todentavia kysymyksiä on yhteensä 63. Ne jakaantuvat yhdeksään eri osa-alueeseen, joita ovat:

1) Turvallisuuspolitiikka, turvallisuustoimintaa ohjaavat periaatteet ja määrittelyt
2) Turvallisuuden vuotuinen toimintaohjelma
3) Turvallisuuden tavoitteiden määrittely
4) Riskien tunnistus, arviointi ja kontrollit
5) Turvallisuusorganisaatio ja vastuut
6) Onnettomuudet, vaaratilanteet, turvallisuuspoikkeamat ja ennalta ehkäisevät toimenpiteet
7) Turvallisuusdokumentaatio ja sen hallinta
8) Turvallisuuskoulutus, tietoisuuden lisääminen ja osaaminen
9) Raportointi ja johdon katselmukset

Turvallisuusauditoinnin tuloksista on laadittu tähän tulosanalyysi, jonka tehtävänä on kartoittaa auditointiraportin tuloksia ja tehdä niistä tarvittavia johtopäätöksiä turvallisuusjohtamisen tasosta. Ensimmäiseksi analysoidaan ne tulokset, jotka sisälsivät poikkeaman. Nämä tulokset eivät täyttäneet KATAKRIn asettamaa suojaustasovaatimusta. Toisena analyysin kohteena ovat tulokset, jotka osittain saavuttavat suojaustasovaatimuksen. Nämä tulokset ovat merkitty lieviksi poikkeamiksi. Tämän osion tarkoituksena on arvioida niitä tekijöitä, minkä vuoksi tasoa ei saavutettu ja minkä asian tai toiminnon kehittäminen riittäisi suojaustason saavuttamiseen. Lopuksi analysoidaan tulokset, jotka eivät sisältäneet poikkeamaa eli joissa vaadittu suojaustaso täytettiin. Tämän osion tarkoituksena on arvioida, mitkä asiat tai toiminnot ovat yksikössä sellaisia, että ne riittävät suojaustason saavuttamiseen.

Kuviossa 1 on havainnollistettu turvallisuusjohtamisen tason todentamisen tulokset. Suojaustasoista selkeitä poikkeamia sisälsi 28 % vaatimuksista. Lähes puolet, 46 % vaatimuksista olivat lieviä poikkeamia. Korotetun suojaustason täytti 25 % eli neljännes vaatimuksista.



Kuvio 1: Turvallisuusauditoinnin tulosanalyysi

4.1 Poikkeamat

Poikkeaman kaltaiseen tilaan arvioitiin 18 suojaustason kohtaa 63:sta. Tämä tarkoittaa sitä, että 28 % KATAKRIn suojaustason vaatimuksista eivät täyty. Toisin kuin lievissä poikkeamissa, poikkeaman kaltaiset suojaustason tilat vaativat jo hieman enemmän panostusta, jotta KATAKRIn vaatimus saavutettaisiin.

Yksi merkittävä poikkeama on yksikön puuttuva tavoitteellisuus turvallisuustoiminnassa. Esimerkiksi turvallisuusdokumentaatioihin ei ole asetettu turvallisuustoiminnalle tavoitteita, vastuita tai aikatauluja. Tavoitteellisuus turvallisuusasioissa tulee olla luonnollinen osa turvallisuusjohtamista ja niiden tulee olla mitattavissa. Koska tavoitteita ei löydy dokumentoituna, ei niille voi näin asettaa aikataulua eikä vastuuhenkilöitä. Näin myöskään kokonaisturvallisuuteen liittyviä seurantatilastoja ei ole saatavilla.

Dokumentaatioihin kohdistuvan tarkastustoiminnan laatu herättää myös kysymyksiä. Pelastussuunnitelman osalta näkyy tarkastuspäivämäärämerkintöjä, mutta tarkastukset eivät ole johtanut sellaisiin toimenpiteisiin, jotka päivittäisivät suunnitelman vaatimusten ja lainsäädännön mukaisesti.

Yksikön tietoturvasuunnitelma on nimellisesti mukana pelastussuunnitelmassa. Se on kuitenkin sisällöltään todella vaatimaton sisältäen esimerkiksi vain yhden vaaratekijän kohdistuvan tietojen käsittelyyn. Luottamuksellisten tietojen ja henkilötietojen käsittelyyn viitataan vain menettelemään ”ohjeen mukaan” ilman tietoa siitä, mistä ohjeesta on kyse. Vaatimustenmukaista suunnitelmaa ei siis ole olemassa yksikkötasolla. Teknistä tietoturvallisuutta toteuttaa erillinen virasto, jolla on omat ohjeistuksensa yksikön tietoturvallisuuden toteuttamiseksi.

Turvallisuusriskejä ei arvioida kokonaisvaltaisesti, säännöllisesti eikä johdetusti. Ne eivät perustu olemassa oleviin riskianalyysimenetelmiin eikä niitä dokumentoida. Riskien arvioinnit perustuvat lähinnä tilanne- ja tapauskohtaisiin arviointeihin. Vaikka riskien arviointi ei olekaan järjestelmällisesti dokumentoitua, turvallisuuskoulutuksessa se muodostuu kouluttajien väliseen keskusteluun. Turvallisuuskoulutuksen lisääminen kohonneessa turvallisuusriskissä perustuu lähinnä yksittäisten toimijoiden aktiivisuuteen. Myöskään tietoturvariskien arviointi ja mittaaminen eivät ole järjestelmällistä. Tietoturvallisuutta korostetaan ja siihen puututaan lähinnä tietoturvarikkomusten jälkeisissä jälkipuinneissa. Ennalta ehkäisevää toimintaa tietoturvarikkomusten varalta ei ole jalkautettu kentälle, vaikka ohjeita löytyykin runsaasti. Turvallisuuskoulutuksen tasovaatimuksia eri henkilöstöryhmille kuitenkin suunnitellaan tietoturvallisuuden osalta.

4.2 Lievät poikkeamat

Suojaustason osittainen tai puutteellinen saavuttaminen on merkitty auditointiraporttiin lieväksi poikkeamaksi. KATAKRIn mukaisen suojaustason saavuttaa siis osittain 29 kohtaa 63:sta. Kyseessä on melkein puolet, noin 46 % kysymyssarjan vaatimuksista. Monet lievät poikkeamat pystyttäisiin yksikössä korjaamaan vaatimustenmukaiseksi pienelläkin korjauksella. Ainoastaan jo dokumentoinnin parantaminen nostaisi huimasti lieviä poikkeamia suojaustason mukaiselle tasolle.

Viranomaisyksikölle ominaisesti monet toimialaan liittyvät lait ja asetukset olivat pääsääntöisesti KATAKRIn mukaisella mallilla. Myös eri turvallisuuslainsäädäntöjen vaatimukset tunnetaan teoriatasolla ja ne tiedostetaan hyvin. Tästä huolimatta yksikön pelastussuunnitelmaa ei ole päivitetty ajan tasalle uuden pelastuslain kanssa. Turvallisuuslainsäädännön seuraamiselle on myös määritetty vastuuhenkilö, joka saa vuosittain täydennyskoulutuksen ohella tietoa turvallisuuslainsäädännön muutoksista. Turvallisuuskoulutuksissa annetaan lainsäädännöllistä perustaa annettavalle koulutukselle, mutta yleisesti henkilökunnan tietoisuuteen turvallisuuslainsäädäntöä tai sen muutoksia jalkautetaan kuitenkin huonosti. Esimerkiksi uudelle työntekijälle ei ole annettu lainkaan tietoturvakoulutusta, vaikka organisaation ja hallinnonalan tasolla on olemassa yksityiskohtaisia, viranomaistason ohjeistuksia tietojen käsittelyyn.

Käytännössä yksikkötason tietoturvakäytäntöjen noudattaminen, kouluttaminen ja toteuttaminen ovat puutteellista ja hajanaista. Teknistä tietoturvallisuutta koordinoidaan organisaatiossa erillisen viraston ohjauksessa, joka vastaa teknisten tietoturvariskien tunnistamisesta ja arvioinnista. Henkilökuntaa kehotetaan yleisesti käsittelemään suojattavaa aineistoa vaatimustenmukaisella tavalla, mutta käytännön ohjeistusta tai dokumentointia ei tähän ole kuitenkaan yksikkötasolla olemassa. Tietoturvapoikkeamatilanteisiin henkilöstöä ohjeistetaan pääsääntöisesti sähköisessä muodossa. Ohjeistukset eivät tule konkreettisesti ilmi, koska niitä ei jalkauteta käytäntöön eikä harjoitella.

Yksiköllä ei ole toimintasuunnitelman yhteyteen laadittua turvallisuuden toimintaohjelmaa. Uuden pelastuslain (2011) tasalle päivittämättömät pelastussuunnitelma ja turvallisuussuunnitelma kuitenkin löytyvät. Myös osa suunnitelmiin sisällytetyistä vastuuhenkilöistä ovat jo jääneet eläkkeelle tai muuten vaihtuneet. Dokumentoidut, turvallisuuteen liittyvät suunnitelmat ovat yleisohjeita, vaikka eri sidosryhmissä tulisi ottaa huomioon erilaiset turvallisuustavoitteet ja – tarpeet myös dokumentoidusti. Ylimmän johdon tasolla ymmärretään, että toimintaohjelmaa tulisi päivittää paremmin ja se tulisi liittää yksikön vuosittaiseen toimintasuunnitelmaan.

Turvallisuuden johtaminen yksikössä kattaa pelastus-, varautumis- ja tietoturvasuunnitelmaan sisältyvät osa-alueet tila-, tieto- ja henkilöstöturvallisuudesta. Turvallisuusjohtamisen organisoinnissa oli epäselvyyksiä. Yksikössä on tehtävänkuvauksessa määritelty yksi strategisesta turvallisuusjohtamisesta vastaava, joka kuuluu ylimpään johtoon. Tämän lisäksi yksikössä oli myös turvallisuudesta vastaava esimies, jonka vastuulla oli operatiivinen turvallisuusjohtaminen. Käytännössä myös strateginen turvallisuusjohtaminen oli vastuutettu turvallisuudesta vastaavalle esimiehelle. Yksikön johtajan vastuuta kokonaisturvallisuuden johtamisesta ei havaittu dokumentoituna ja näin turvallisuusjohtamisjärjestelmästä puuttui dokumentoitu ylimmän johdon osuus sekä tarkka vastuun määrittely.

Yksikössä ei tunnisteta, arvioida eikä hallita turvallisuusriskejä kokonaisvaltaisesti ja järjestelmällisesti. Erityisesti riskien arvioinnin puutteellisuuden ja vajavaisuuden vuoksi niiden vaikutusta ei voida kattavasti mitata KATAKRIn riskien tunnistus, arviointi ja kontrollit – osa-alueella. Koska arviointi ei ole järjestelmällistä eikä kokonaisvaltaista, riskejä arvioidaan hajanaisesti ja tapauskohtaisesti. Mikäli tapauskohtainen riskienarviointi tehdään, se otetaan huomioon organisaation tavoitteissa. Tavoitteiden toteuttamisessa on kuitenkin vajavaisuuksia talousresurssien puutteiden vuoksi.

Yksikön tärkeät kohteet ja toiminnot on tunnistettu käytännön ja hiljaisen tiedon tasolla, mutta itse tunnistusprosessia ja sen tuloksia ei ole dokumentoitu. Suojattaville kohteille on määritelty vastuuhenkilöt, mutta niitä ei ole päivitetty ajan tasalle. Suojattavien kohteiden riskejä hallitaan aliurakoitsijoista ja palveluntarjoajista tehdyllä suppealla turvallisuusselvityksellä. Suppea turvallisuusselvitys on karkeasti kohdistettu tilaturvallisuuteen liittyvien riskien hallintaan eikä niinkään tietoturvariskeihin. Poikkeavissa tilanteissa riskien arviointia pidetään jatkuvasti ajan tasalla. Niihin riskien arviointi on koulutettu esimiestasolla ja siihen on olemassa ohjeistus.

Turvallisuustoimintaa ohjaavat dokumentaatiot ovat jatkuvasti saatavilla yksikön sisäisessä verkossa ja kirjallisena. Turvallisuusdokumentaatioiden saatavuudesta ja päivityksestä ei tiedoteta työntekijöille riittävästi eikä niiden sisältöä kerrata muun koulutuksen yhteydessä. Turvallisuusdokumentaatioiden tuottaminen, päivittäminen ja vaatimustenmukaisuus eivät täyttäneet KATAKRIn vaatimuksia. Turvallisuusdokumentaatiot ovat kuitenkin kohdistettu ja suunniteltu yksikköä varten. Niiden noudattaminen ja niihin sitoutuminen eri työntekijätasoilla perustuu lähinnä nimelliseen vastuuseen virkavastuun myötä, eikä noudattamisen valvontaa suoriteta vaatimustenmukaisesti. Esimiestasolla turvallisuuden toteuttamista kuitenkin valvotaan, mutta niiden tuloksia ei dokumentoida.

Vaativiin ja poikkeaviin tilanteisiin on yksiköllä olemassa dokumentoidut toimintamallit ja niihin on esimiestasolla saatu kattava koulutus. Poikkeamatilanteita ei ole vielä harjoiteltu kattavasti työntekijätasolla eikä niitä harjoitella säännöllisesti koko yksikössä.

Yksikön turvallisuusorganisaatio muodostuu niin, että turvallisuuden eri osa-alueisiin on nimetty henkilöt ja vastuu on määritelty henkilön tehtävänkuvauksessa. Vastaavia henkilöitä koulutetaan myös omaan vastuualueeseensa. Tällä hetkellä yksiköltä puuttuu kuitenkin tietoturvasta vastaava henkilö. Myös turvallisuusorganisaation näkyvyys ja tietoisuus henkilökunnan keskuudessa on heikkoa, koska esimerkiksi uusi työntekijä ei osannut tunnistaa turvallisuusjohtamisjärjestelmää.

Yksikön turvallisuustekniset resurssit ovat osittain puutteellisia ja turvallisuuskriittisillä työalueilla henkilöstöresurssit ovat vähäistä. Turvallisuustyöstä vastaavia kuitenkin koulutetaan hyvin omille osa-alueilleen ja vaadittava pohjakoulutus tiettyihin tehtäviin edellyttää normaalia kattavampaa turvallisuuskoulutusta. Vaikka tekniset resurssit ovat osittain puutteellisia, turvallisuuspoikkeamien havainnointia varten yksiköllä on tekniset valmiudet havainnoida turvallisuuspoikkeamia (palohälytys-, murtohälytys- ja kameravalvontajärjestelmät). Henkilökunta myös raportoi turvallisuuspoikkeamista suullisesti ja osittain sähköpostin välityksellä. Raportoiminen on tilannesidonnaista ja poikkeamien dokumentoinnissa parantamisen varaa.

Turvallisuusjärjestelmän seurantatarkastukset ovat osa yksikön jatkuvaa toimintaa. Seurantaa ei kuitenkaan dokumentoida. Seurannan turvallisuuteen kohdistuvia tilastoja analysoidaan enemmälti henkilöstö- ja työturvallisuuden osa-alueilla. Muiden turvallisuuden osa-alueilta ei ole dokumentoitua seurantaraporttia. Turvallisuusdokumentteja säilytetään niille kuuluvassa paikassa kirjallisena ja niitä on saatavissa myös sähköisenä yksikön sisäisestä verkosta.

Turvallisuuskoulutukseen ei ole säädetty tasovaatimuksia ja näin ollen niitä ei löydy dokumentoituna. Koulutusvaatimusten täyttymistä kuitenkin arvioidaan ja seurataan kouluttajien taholta aina koulutuksen yhteydessä. Kouluttajilla on myös vahva käsitys tehtävien vaatimustenmukaisuudesta. Kyseinen seuranta ja käsitys tulisi myös dokumentoida, jotta sitä pystyttäisiin myös kehittämään tarkoituksenmukaisempaan suuntaan. Tietoturvakoulutus ei täytä KATAKRIn tasovaatimuksia. Tietojenkäsittelypalveluihin ja tietojen käsittelyyn on olemassa ohjeita mutta niitä käydään läpi oikeastaan vain sähköpostitasolla eikä niitä jalkauteta käytännön tasolla. Tietojen käsittelyyn liittyvää koulutusta ollaan kuitenkin järjestämässä.

4.3 Täyttyneet vaatimukset

KATAKRIn hallinnollisen turvallisuuden kysymyssarjan 63 suojausvaatimuksesta 16 täyttää asetetun suojaustason eli poikkeamaton osuus on 25 prosenttia. Suojaustason voidaan katsoa täyttyneen monissa sellaisissa tapauksissa, joissa viranomaistoimintaa ohjaava lainsäädäntö tai yksikköä erikseen ohjaavat ja lait asetukset niin määräsivät. Monet viranomaisyksikköä koskevat toimintavelvoitteet ja lakiin perustuvat asetukset koordinoivat turvallisuusjohtamista.

Viranomaistyötä koskevan lainsäädännön myötä yksikön tehtävänkuvauksissa oli selvät määrittelyt turvallisuustyön vastuista ja ne näkyvät myös tehtävänkuvauksissa. Kohteen ylimmällä johdolla on kokonaisvastuu hallinnollisen turvallisuuden toteuttamisesta ja sitoutuminen turvallisuustyön tavoitteisiin. Siitä huolimatta turvallisuudesta vastaavan esimiehen tehtävänkuvauksessa on yksilöity vaikutusmahdollisuus turvallisuustoiminnan kehittämiseen ja johtamiseen. Turvallisuudesta vastaava raportoi myös eteenpäin turvallisuuteen liittyviä asioita. Ra-

portointi on myös vuorovaikutteista: organisaation johdosta raportoidaan olennaisia asioita myös turvallisuudesta vastaavalle.

Yksikön menettelyt poikkeaviin häiriötilanteisiin täytti hyvin KATAKRIn vaatimukset. Yksiköllä on selkeä menettely jatkuvuudenhallintaan. Se on määrittänyt erikseen henkilöt, jotka vastaavat poikkeamatilanteisiin varautumisesta, suunnittelusta ja niihin kouluttamisesta. Viranomaisyksikön ominaisuudessa vastuut varautumisen osalta ovat ennalta määriteltyjä ja osa perustehtävää. Myös yksikön turvallisuustoimenpiteet resursoidaan tarkoituksenmukaisesti, koska niiden tarkastelu ottaa huomioon taloudellisuuden ja tehokkuuden.

Vaikka dokumentoinnissa oli yksiköllä puutteita monella osa-alueella, oli henkilökunnalle annettu turvallisuuskoulutus dokumentoitu KATAKRIn suojaustason mukaisesti. Henkilöstön täydennyskoulutuksessa läpikäydään yksikköön kohdistuvia turvallisuusriskejä ja niitä nostetaan esille myös perehdytysvaiheessa. Täydennyskoulutuksessa on huomioitu myös, että yksikön tiettyjen henkilöstöryhmien pohjakoulutukseen kuuluu turvallisuusriskeihin perehtyminen. Näin koulutus muokataan kullekin henkilöstöryhmälle tarkoituksenmukaisesti.

Teknisiä tietoturvarikkomuksia seurataan yksikköä ylemmällä organisaatiotasolla. Mikäli rikkomuksia havaitaan, virkamieslaissa on rikkeiden käsittelystä ja seurauksista omat seuraamukset sekä menettelyt. Mikäli tietoturvarikkeitä ylipäätään havaitaan yksikössä, niihin pyritään puuttumaan ainakin esimiestasolla ja ne myös käsitellään asianmukaisesti rikkeen vakavuudesta riippuen.

Turvallisuusjärjestelmän toimivuutta tarkastellaan jatkuvasti. Järjestelmän seuranta on aktiivista ja vaikuttaa turvallisuussuunnitteluun. Yksikössä järjestetään säännöllisesti turvallisuuspalavereita, minkä tarkoituksena on kehittää yleistä turvallisuutta. Sen jäsenistö koostuu muutamasta työntekijästä ja yhdestä ylimmän johdon jäsenestä. Palavereissa käydään läpi yksikössä havaittuja turvallisuusriskejä ja – poikkeamia. Turvallisuuspalavereissa käydyt asiat dokumentoidaan ja ne ovat kaikkien saatavilla.

5 Kehittämisehdotukset

Organisaation turvallisuuden kehittämissuunnitelma kuvaa lyhytaikaista, noin vuoden mittaista ohjausta turvallisuuden toteuttamiseksi. Kehittämissuunnitelmassa tulee kuvata mahdollisimman tarkasti turvallisuuden kehittämiskohteet, painotusalueet, aikataulu ja vastuuhenkilöt. Suunnitelma tulee hyväksyttää ja vahvistaa organisaation ylimmällä johdolla. Turvallisuuteen liittyvät ohjeistukset ohjaavat myös organisaation turvallisuutta. Niiden tulee jokaisen työntekijän ymmärrettävissä ja saatavilla. (Miettinen 2002, 59)

Tässä opinnäytetyössä ei tehdä sen kohteelle turvallisuuden kehittämissuunnitelmaa. Tarkoituksena on kuitenkin antaa sellaisia turvallisuuden kehittämisehdotuksia, joiden pohjalta kohdeyksikkö voi alkaa kehittämissuunnitelmaa rakentamaan. Seuraavat kehittämisehdotukset sisältävät suosituksia turvallisuuden toimintaohjelman ja turvallisuustavoitteiden laadintaan sekä ohjeita turvallisuusorganisaation, kokonaisvaltaisen riskienhallinnan, turvallisuuskoulutuksen ja turvallisuusdokumentaatioiden toteuttamiseen.

Turvallisuusjohtamisen toteuttamisen perustana on erillinen turvallisuuden toimintaohjelma. Toimintaohjelman tulisi olla luonnollinen osa organisaation toimintasuunnitelmaa sisältäen laaditut turvallisuustavoitteet. Tavoitteiden tulisi sisältää aikataulu, mitä yksikön olisi noudatettava. Tavoitteiden asettamisen ja aikataulutuksen lisäksi jokainen turvallisuuden osa-alueelle tulee määrittää vastuuhenkilö. Vastuuhenkilö huolehtisi omalta osa-alueeltaan siitä, että turvallisuustavoite pyritään saavuttamaan aikataulun mukaisesti. Turvallisuuden toimintaohjelmaa tulisi kouluttaa organisaation henkilöstölle ja se tulisi perehdyttää myös uusille työntekijöille.

Organisaation turvallisuusjohtamisjärjestelmään kuuluu toimiva turvallisuusorganisaatio. Sen tulee kattaa vähintään KATAKRIn turvallisuusjohtamisen, fyysisen turvallisuuden, henkilöstöturvallisuuden ja tietoturvallisuuden osa-alueet. Organisaation ylimmän johdon vastatessa kokonaisturvallisuuden johtamisesta, on myös jokaisella turvallisuuden osa-alueella oltava vastuuhenkilö. Vastuuhenkilöllä tulee olla riittävä osaaminen, koulutus ja soveltuvuus sekä resurssit oman osa-alueensa kehittämiseen. Turvallisuusorganisaatio tulee dokumentoida organisaation turvallisuuden toimintaohjelmiin ja turvallisuussuunnitelmiin. Turvallisuusorganisaatio tulee perehdyttää uusille työntekijöille ja sitä tulee päivittää henkilöstömuutosten jälkeenkin.

Turvallisuusjohtamisen pohjana toimii kokonaisvaltainen turvallisuusriskien arviointi. Sen on oltava organisaatiossa jatkuva prosessi. Riskien arviointiin kuuluu, että riskit tunnistetaan, analysoidaan ja niiden merkitys arvioidaan. Riskien arviointi kuuluu kokonaisvaltaiseen riskienhallintaan, jossa huomioidaan organisaation toimintaan vaikuttavat olennaisimmat tekijät. Auditoitavassa yksikössä riskejä arvioitiin irrallisesti ja tapauskohtaisesti. Kokonaisvaltaisessa riskienhallinnassa noudatetaan päinvastaista logiikkaa. Siinä on tärkeätä arvioida riskejä suhteessa poikkeamiin ja vahinkoihin niin, että riskienhallinnan prosessit, raportointi ja riskienhallintatoimet on yhdistetty organisaation koko toimintaan. (Ilmonen, Kallio, Koskinen & Rajamäki 2010, 47)

Ilmonen ym. mukaan kokonaisvaltaisessa riskienhallinnassa tunnistetaan potentiaaliset riskit, jotka ovat sekä kielteisiä että myönteisiä. Myönteisten riskien tunnistaminen on tärkeää, koska ne vahvistavat organisaation valmiita arvoja sekä kumoavat kielteisten riskien vaikutuksia.

Riskienhallinta tulee kytkeä myös organisaation strategiseen suunnitteluun, jotta sen liiketoimintamahdollisuudet saisivat siitä kaiken hyödyn. Kokonaisvaltaisuuden asema riskienhallinnassa täyttyy, mikäli koko organisaatio osallistuu sen toteuttamiseen ja riskienhallinta kattaa organisaation jokaiset mahdollisuudet ja riskit (2010, 47-48).

Turvallisuuskriittisen organisaation velvollisuus on huolehtia henkilökuntansa riittävästä koulutuksesta ja osaamistasosta. Koulutus on avainasemassa organisaatioturvallisuuden ylläpitämisessä. Turvallisuuskulttuurin rakentumiseen vaikuttaa työntekijöille annettava koulutus, mikäli siinä huomioidaan ja korostetaan turvallisia toimenpiteitä kaikessa toiminnassa (Reiman & Oedewald 2008, 76)

Henkilökunnan turvallisuuskoulutuksen tulee pohjautua osittain turvallisuusriskien arviointeihin. Riskien arviointien myötä koulutusresursseista tulee oikein suhteutettuja ja niistä saadaan sekä taloudellisia että tehokkaita. Turvallisuuskoulutus on yksikössä hyvin toiminnallista. Vaikka teoriakoulutusta lainsäädännön osalta koulutukseen sisältyykin, kokonaisturvallisuuden ja yksikön turvallisuuspolitiikan lisääminen käsitteeksi tukisi hyvin nykyisen kaltaista koulutusta. Kokonaisuuden hahmottaminen toimisi myös motivoivana tekijänä koulutukseen osallistumiselle. Niin kuin yksikön koko turvallisuustoiminnan, myös turvallisuuskoulutuksen tulisi olla tavoitteellisempaa. Koulutuksessa tulisi lisätä tasovaatimukset ja niiden täyttymistä tulisi valvoa kouluttajien osalta.

Organisaation turvallisuustoiminta tulisi dokumentoida järjestelmällisesti. Dokumentaation pohjalta tulisi olla todennettavissa tehdyt toimenpiteet ja velvollisuudet turvallisuustoiminnan eteen. Organisaation turvallisuustoimintaa pystytään myös ohjaamaan dokumentteihin kirjattujen toimintamallien mukaan. Dokumentointi auttaisi myös turvallisuustason todentamista (Paasonen ym. 2012, 171). Turvallisuusjohtamisen tason todentaminen ei olisi onnistunut, mikäli auditointi olisi jätetty pelkästään kohteen dokumenttien varaan. Turvallisuusdokumentointi oli yksi suurimmista kehittämisen alueista kohteessa. Sen tulisi olla osa turvallisuusjohtamista kaikilla turvallisuuden osa-alueilla. Turvallisuusdokumentaatiot kuvaavat muun muassa organisaation turvallisuusstrategisia päämääriä, toimintamalleja, ohjeistuksia, ja laatujärjestelmiä ym. Vaikka dokumentaatiot eivät yksinään riitä toteuttamaan turvallisuutta, ne toimivat pohjana koko turvallisuustoiminnalle.

6 Yhteenveto

Tämän laadullisen opinnäytetyön tavoitteena oli todentaa turvallisuusjohtamisen taso eräässä suomalaisen turvallisuusorganisaation viranomaisyksikössä. Tutkimusongelmina olivat kohteen turvallisuusjohtamisen taso ja Kansallisen auditointikriteeristö KATAKRIn käytettävyys viranomaisyksikössä. Turvallisuusjohtamisen taso todennettiin auditoimalla kohde vertaamalla KATAKRIn Hallinnollisen turvallisuuden osiota vallitsevaan tasoon.

Opinnäytetyön kohteena toimi Etelä-Suomessa sijaitseva suomalainen turvallisuusviranomaisyksikkö, joka työllistää noin 150 henkilöä. Yksikkö on osa isompaa, valtakunnallista turvallisuusorganisaatiota, joka työllistää yhteensä noin 3000 henkilöä. Tämän kvalitatiivisen tutkimuksen tutkimuslajina käytettiin hermeneuttista menetelmää, jonka periaatteena on oppia ymmärtämään kohteessa tutkittavaa kokonaisuutta. Hermeneutiikassa ennakkoluulot ja omat mielikuvat ovat osa auditoitavan kohteen ymmärtämisen kehittymistä. Kohdetta tarkastellaan kokonaisuutena ensin ennakoivasti, jonka jälkeen sitä yksityiskohtaisesti tutkitaan. Tiedonkeruumenetelminä käytettiin dokumenttientarkastelua, strukturoituja haastatteluja ja havainnointia.

Ensimmäisenä osana opinnäytetyön teoriapohjaa ja keskeisenä käsitteenä toimi Kansallinen turvallisuusauditointikriteeristö KATAKRI. Toisena tärkeänä käsitteenä on turvallisuusjohtaminen. Teoriapohjassa kerrotaan turvallisuusjohtaminen historiaa Suomessa, turvallisuuspolitiikan ja turvallisuuskulttuurin määritelmää sekä turvallisuusjohtamisjärjestelmän kokonaisuutta. Teoriapohjassa kytketään myös olennainen turvallisuus ja taloudellisuus yhteen. Myös riskienhallintaa turvallisuusjohtamisen työkaluna käydään läpi riskien tunnistamisen, analysoinnin ja riskien hallinnan kautta. Lopuksi avataan itse auditoinnin käsitettä ja sen eri muotoja.

Kohde auditoitiin käyttäen KATAKRIn hallinnollisen turvallisuuden korotetun tason suojausvaatimuksia. Auditoinnista tehtiin raportti, jonka perusteella laadittiin tulosanalyysi. Raportin tulokset merkittiin niin, että havaitut poikkeamat eroteltiin punaisella, lievät poikkeamat keltaisella ja saavutetut suojaustasovaatimukset vihreällä värillä. Suojaustasoista selkeitä poikkeamia sisälsi 28 % vaatimuksista. Lähes puolet, 46 % vaatimuksista olivat lieviä poikkeamia ja Korotetun suojaustason saavutti 25 % eli neljännes vaatimuksista.

Poikkeaman kaltaiseen tilaan arvioitiin 18 suojaustason kohtaa 63:sta. Yksi merkittävä poikkeama oli yksikön puuttuva tavoitteellisuus turvallisuustoiminnassa, joka näkyi puuttuvissa tavoitteissa, vastuuttamisessa tai aikataulutuksessa. Myös dokumentaatioiden laatu oli osittain huonoa. Poikkeama oli myös yksikön tietoturvajohtamisessa riskien arvioinnin ollessa vaatimatonta. Turvallisuusriskejä ei arvioida kokonaisvaltaisesti, säännöllisesti eikä johdetusti. Turvallisuusjohtaminen ei ole riskiperusteista, joten nykyaikainen riskien arvioinnin osuus on

yksikössä lähes olematonta. Riskejä ei arvioida myöskään tietoturvallisuuden osalta eikä tietoturvarikkomuksia ennalta ehkäistä jalkauttamalla siihen liittyvää koulutusta.

Lieviä poikkeamia merkittiin 29 kohtaa 63:sta. lievät poikkeamat pystyttäisiin yksikössä korjaamaan vaatimustenmukaiseksi pienelläkin korjauksella. Ainoastaan jo dokumentoinnin parantaminen nostaisi huimasti lieviä poikkeamia suojaustason mukaiselle tasolle. Viranomaisyksikölle ominaisesti monet toimialaan liittyvät lait ja asetukset olivat pääsääntöisesti KATAKRIn mukaisella mallilla esimerkiksi turvallisuuskoulutuksissa. Muuten henkilökunnan tietoisuuteen turvallisuuslainsäädäntöä tai sen muutoksia jalkautetaan kuitenkin huonosti. Yksikössä tietoturvakäytäntöjen noudattaminen, kouluttaminen ja toteuttaminen ovat puutteellista ja hajanaista. Ohjeistuksia on olemassa, niitä ei jalkauteta käytäntöön eikä harjoitella. Yksiköllä ei ole toimintasuunnitelman yhteyteen laadittua turvallisuuden toimintaohjelmaa. Turvallisuusjohtamisen organisoinnissa oli epäselvyyksiä ja turvallisuusjohtamisjärjestelmästä puuttui dokumentoitu ylimmän johdon osuus sekä tarkka vastuun määrittely.

Turvallisuustoimintaa ohjaavat dokumentaatiot ovat jatkuvasti saatavilla yksikön sisäisessä verkossa ja kirjallisena, mutta niiden tuottaminen, päivittäminen ja vaatimustenmukaisuus eivät täyttäneet KATAKRIn vaatimuksia. Vaikka yksikön turvatekniset resurssit ovat osittain puutteellisia, niillä pystytään vajavaisesti havainnoimaan turvallisuuspoikkeamia. Turvallisuuskoulutukseen ei ole säädetty tasovaatimuksia, mutta niiden toteutumista valvotaan silmämääräisesti kouluttajien taholta.´

KATAKRIn 63 suojausvaatimuksesta 16 täyttää asetetun suojausvaatimuksen yksikössä. Tehtävänkuvaukset ja vastuut olivat määriteltyjä. Yksikön menettelyt poikkeaviin häiriötilanteisiin täytti KATAKRIn vaatimukset. Yksiköllä on myös selkeä menettely jatkuvuudenhallintaan ja se on määrittänyt erikseen henkilöt, jotka vastaavat poikkeamatilanteisiin varautumisen suunnittelusta. Turvallisuustoimenpiteet resursoidaan yksikössä tarkoituksenmukaisesti, koska niiden tarkastelu ottaa huomioon taloudellisuuden ja tehokkuuden. Henkilökunnalle annettu turvallisuuskoulutus oli dokumentoitu. Turvallisuusjärjestelmän toimivuutta tarkastellaan jatkuvasti. Sen seuranta on aktiivista ja vaikuttaa turvallisuussuunnitteluun.

Tulosanalyysista saaden arvioinnin perusteella laadittiin kohteelle turvallisuustoiminnan kehittämisehdotuksia mahdollista kehittämissuunnitelmaa varten. Kehittämisehdotukset sisälsivät suosituksia turvallisuuden toimintaohjelman ja turvallisuustavoitteiden laadintaan sekä ohjeita turvallisuusorganisaation, kokonaisvaltaisen riskienhallinnan, turvallisuuskoulutuksen ja turvallisuusdokumentaatioiden toteuttamiseen. Auditointiraportin ja tulosanalyysin perusteella voidaan todeta, että auditoitavan kohteen turvallisuusjohtamisen taso ei pystynyt saavuttamaan KATAKRIn korotetun tason vaatimusta hallinnollisesta turvallisuudesta. Kohteen suojaustasovaatimukset täyttyivät enintään KATAKRIn perustason osalta.

7 Oman työn arviointi

Turvallisuuden johtaminen on luonnollinen osa kokonaisjohtamista, josta vastaa organisaation ylin johto. Turvallisuusjohtamiseen kuuluvat olennaisena osana järjestelmällisyys, tavoitteellisuus, tehokkuus, kokonaisvaltaisuus ja dokumentointi. Perinteisesti ”turvallisuusjohtamiseen” on yleisesti kuulunut, että lakisääteiset turvallisuusasiat hoidetaan pääsääntöisesti hyvin ja turvallisuuspoikkeamiin puututaan vain silloin kun jotain on jo tapahtunut. Tässäkin kohteessa valitettavasti poikkeamiin ja vahinkoihin on puututtu tällä perinteisellä tavalla. Ongelma on riskiperusteisen turvallisuusjohtamisen puuttumisessa. Tämän opinnäytetyön auditointiprosessin myötä saatiin selville, että tässäkin yksikössä riskejä arvioidaan vain tapaus- ja tilannekohtaisesti. Nykyaikaiseen, ennakoivaan ja varautuvaan turvallisuusjohtamisen perustana on riskien arviointi, missä niiden tunnistaminen, analysointi ja hallinta on omaksuttu selkeäksi osaksi.

Lähtöasetelmien mukaiset odotukset turvallisuusjohtamisen tasojen täyttymisestä olivat viranomaisyksikön luonteesta johtuen korkealla. KATAKRI on lähtöisin viranomaisten aloitteesta, joten viranomaisyksikköjen turvallisuustason voisi olettaa olevan kunnossa. KATAKRIn security-näkökulman vuoksi tässä opinnäytetyössä ei kiinnitetty niinkään huomioita safety-näkökulman turvallisuusjohtamiseen. Auditoinnin tulosanalyysin perusteella kohteeseen olisi syytä tehdä myös paloturvallisuuteen ja pelastustoimintaan liittyvä katselmus. Yksikön safety-näkökulman turvallisuustasoa voisi kehittää esimerkiksi Euroopan laatupalkintomalliin (EFQM) perustuvan ja Keski-Uudenmaan Pelastuslaitoksen kehittämän Tutor-riskienarviointimallin avulla (Keski-Uudenmaan Pelastuslaitos 2012). Jatkotutkimusaiheina voisi olla myös muut KATAKRIn auditointiprosessiin kuuluvat osa-alueet (henkilöstö-, fyysinen ja tietoturvallisuus).

KATAKRI-auditoinnin tuominen viranomaisympäristöön tuntui aluksi hyvin haastavalta, mutta niiden kysymykset olivat kuitenkin hyvin sovellettavissa kohteen toimintaympäristön piiriin kuuluville havainnoille ja tiedoille. Tämä edellyttää sitä, että auditoija tekee riittävästi taustatyötä etenkin ennen auditointihaastatteluja. Vaikka KATAKRIn kysymykset sopivatkin strukturoituihin haastatteluihin, pelkästään niiden varaan jääminen ei riitä varsinkaan sellaisissa tapauksissa, joissa kohde ei ole aikaisemmin tutustunut riittävästi KATAKRIin. Silloin auditoijan tulee selvittää, mitä kullakin kysymyksellä tarkoitetaan auditoitavassa kohteessa ja osata kohdentaa ne tarvittavaan kontekstiin. KATAKRIlla auditoiminen edellyttää vahvaa turvallisuusasiantuntijuutta ja kokonaisymmärrystä organisaatioturvallisuudesta.

Tiedonkeruumenetelmät (dokumenttien tarkastelu, haastattelut ja observointi) sopivat hyvin turvallisuusauditointityöhön. Haasteita kysymysten asettelussa ja tiedon keräämisessä oli kohteen ennalta tietämättömyys KATAKRIn olemassaolosta. Toisaalta tietämättömyys saattoi luoda autenttisuutta erityisesti haastattelu- ja havainnointiprosesseihin. Auditointiprosessi kärsi

eniten dokumentoinnin puutteesta, sillä ainoastaan niihin nojautuva auditointi olisi jäänyt todella vajavaiseksi. Haastattelujen ja havainnointien myötä sai kuitenkin selville paljon sellaisia turvallisuuteen liittyviä asioita, joita hoidetaan hiljaisen tiedon tai käytänteiden avulla.

Opinnäytetyöhön kuulunut auditointityö toimi yksikölle hyvänä esiauditointina. Mikäli yksikölle suoritettaisiin virallinen KATAKRIn mukainen auditointi, tämän auditointiraportin pohjalta siihen pystyttäisiin siihen valmistautumaan paljon paremmin. Myös opinnäytetyön myötä yksikölle saatettu tietoisuus turvallisuusjohtamisesta, turvallisuusauditoinnista ja sen prosessista auttavat tulevaisuudessa valmistautumaan mahdollisiin turvallisuustoiminnan arviointitilaisuuksiin.

Opinnäytetyön tekijälle tämä raportti toimi niin yhteenvetona koko turvallisuusalan koulutusohjelman opintojaksoista kuin vahvistavana tekijänä henkilökohtaisessa turvallisuusasiantuntijuuden kehittämisessä. Turvallisuusjohtamisen tutkimisen yhdistäminen auditointityöhön auttoi tuomaan kriittistä näkökulmaa olemassa oleviin turvallisuuskriteeristöihin. Kohteena ollut viranomaisyksikkö suhtautui toteutettuun auditointitapahtumaan erittäin rakentavasti. Prosessissa esille nousseet turvallisuusjohtamisen poikkeamiin kiinnitettiin yksikössä välittömästi huomiota ja niitä tullaan ylimmän johdon mukaan kehittämään. Tämän perusteella voidaan päätellä, että opinnäytetyöhön kuuluva turvallisuusauditointi antoi yksikölle tilannekuvan nykyisestä turvallisuusjohtamisen tasosta, ymmärrystä toteuttaa riskiperusteista turvallisuustyötä ja perusteet parantaa turvallisuusjohtamisen tasoa.

Lähteet

Carter, N. 2004. Auditointi ja ISO 19011. Helsinki: Gummerus Kirjapaino.

Flink, A-L., Reiman, T. & Hiltunen, M. Heikoin lenkki – Riskienhallinnan inhimilliset tekijät. Helsinki: Edita Prima.

Gadamer, H-G. Hermeneutiikka. 2004. Tampere: Vastapaino.

HE 69/2001. Hallituksen esitys Eduskunnalle laiksi yksityisistä turvallisuuspalveluista sekä eräiksi siihen liittyviksi laeiksi.

Heinonen, J., Keinänen, A. & Paasonen, J. 2013. Turvallisuustutkimuksen tekeminen. Helsinki: Tietosanoma.

Hirsjärvi, S & Hurme, H. 2009. Tutkimushaastattelu. Helsinki: Gaudeamus Helsinki University Press.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. Helsinki: Tammi.

Ilmonen, I., Kallio, J., Koskinen, J. & Rajamäki, M. 2010. Johda riskejä – käytännön opas yrityksen riskien-hallintaan. Helsinki: Kustannusosakeyhtiö Tammi.

Kerko, P. 2001. Turvallisuusjohtaminen. Jyväskylä: PS-kustannus.

Keski-Uudenmaan Pelastuslaitos. 2012. Tutor Turvallisuustoiminnan riskienarviointijärjestelmä. TUKEVA2 Väliseminaari 28.3.2012

Kivelä, A & Sutinen, A. (toim.). 2009. Teoria ja traditio. Turku: Suomen Kasvatustieteellinen seura.

Miettinen, J. E. 2002. Yritysturvallisuuden käsikirja. Helsinki: Talentum Media.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2009. Kehittämistyön menetelmät. Helsinki: WSOY-pro.

Paasonen, J. (toim.), Huumonen, T. & Paasonen, L. 2012. Oppilaitoksen turvallisuusjohtaminen. Helsinki: Tietosanoma.

Pelastuslaki 29.4.2011/379.

Puolustusministeriö. 2011. Kansallinen turvallisuusauditointikriteeristö KATAKRI II.

Reiman, T. & Oedewald, P. 2008. Turvallisuuskriittiset organisaatiot. Helsinki: Edita Publishing.

Simola, A. 2005. Turvallisuuden johtaminen esimiestyönä. Väitöskirjatutkimus. Oulu: Oulun Yliopisto.

Ulkoministeriö. 2011. Kansallinen turvallisuusviranomainen - Turvallisuusviranomaisten käsikirja yrityksille.

Valtiovarainministeriö. 2007. VAHTI - Tietoturvallisuudella tuloksia. Helsinki: Edita Prima.

Vilkka, H. & Airaksinen, T. 2003. Toiminnallinen opinnäytetyö. Helsinki: Kustannusosakeyhtiö Tammi.

Sähköiset lähteet:

Elinkeinoelämän keskusliitto. 2013. Yritysturvallisuuden osa-alueet. Viitattu 19.11.2013. http://www.ek.fi/ek/fi/tyomarkkinat_ym/Yritysturvallisuus/osa-alueet/Osa-alueet.php

Suomen Standardisoimisliitto SFS Ry. 2013. ISO 31000 Riskienhallinta. Viitattu 23.11.2013. http://www.sfs.fi/julkaisut_ja_palvelut/tuotteet_valokeilassa/iso_31000_riskienhallinta

Suomen Standardisoimisliitto SFS Ry. 2013. SFS-EN ISO 19011 Johtamisjärjestelmän auditointiohjeet. Viitattu 23.11.2013. http://sales.sfs.fi/sfs/servlets/ProductServlet?action=productInfo&productID=248581

Julkaisemattomat lähteet:

Apulaisjohtaja 2013. Auditointihaastattelut 25.10.2013 & 28.10.2013. Viranomaisyksikkö.

Pelastussuunnitelma. 2008. Viranomaisyksikkö.

Turvallisuusesimies. 2013. Auditointihaastattelu 12.10.2013. Viranomaisyksikkö.

Turvallisuuskouluttaja. 2013. Auditointihaastattelu 7.10.2013. Viranomaisyksikkö.

Turvallisuusstrategia. 2009. Viranomaisorganisaatio.

Turvallisuussuunnitelma, 2008. Viranomaisyksikkö.

Uusi työntekijä. 2013. Auditointihaastattelu 12.10.2013. Viranomaisyksikkö.

Vaativien tilanteiden ohje. 2007. Viranomaisyksikkö.

Kuviot

Liitteet

Liite 1

VIRANOMAISYKSIKÖN HALLINNOLLISEN TURVALLISUUDEN AUDITOINTIRAPORTTI

Ei poikkeamaa
Lievä poikkeama
Poikkeama

	KYSYMYS	SUOJAUSTASO: KOROTETTU TASO (III)	POIKKEAMA	HAVAINNOT
A 101.0	Onko organisaation johto määrittänyt ja hyväksynyt turvallisuuspolitiikan? Onko politiikka tarkistettu määräajoin?	Organisaatiolla on kirjattuna ylimmän johdon hyväksymä turvallisuuspolitiikka tai vastaava turvallisuustoimintaa ohjaava hyväksytty määrittely.		Viranomaisyksikön ominaisuudessa kohteessa on lakiin perustuvia asetuksia turvallisuuden johtamiseksi. Tämän lisäksi erillisiä ohjeita ja määräyksiä on turvallisuustoimintaan liittyen.
A 102.0	Mitä turvallisuuden osatekijöitä turvallisuuspolitiikka ja/tai turvallisuuden johtaminen organisaatiossa kattaa?	Turvallisuusdokumentaatio sisältää ainakin tila-, tieto- ja henkilöstöturvallisuuden osa-alueet sekä turvallisuuspolitiikassa todetun turvallisuusjohtamisen selkeän organisoinnin.		Pelastus-, varautumis- ja tietoturvasuunnitelmaan sisältyy osa-alueet tila-, tieto- ja henkilöstöturvallisuudesta. Turvallisuusjohtamista ei ole selkeästi organisoitu. Turvallisuusjohtamisjärjestelmästä puuttuu ylimmän johdon osuus ja vastuun määrittely.
A 103.0	Vastaako organisaation turvallisuusdokumentaatio toiminnan ja tuotteiden laajuutta ja toimintatapaa sekä niihin liittyviä turvallisuusriskejä?	Turvallisuusdokumentaatio käsittelee organisaatiota yksilöllisesti ja ottaa huomioon muutokset organisaation toiminnassa		Kohdetta käsitellään yksilöllisesti ja turvallisuusdokumentaatiot on selvästi tähän yksikköön tarkoitettu ja suunniteltu. Dokumentaatiossa huomioidaan muuttuvat tilanteet yksikön toiminnassa lakien ja asetusten osalta. Riskien arvioinnin vaikutusta ei kuitenkaan voida mitata sen puutteellisuuden ja vajavaisuuden vuoksi.
A 104.0	Toimivatko organisaation kaikki tasot turvallisuuspolitiikan mukaisesti?	Organisaatiolla on selvä ohjelma valvoa turvallisuuspolitiikan perusteiden mukaista toimintaa. Valvonnan tulokset ovat esitettävissä.		Yksiköllä on nimellinen vastuu perusteiden valvomiseen. Valvontaa ei kuitenkaan suoriteta vaatimustenmukaisesti. Esimiestasolla turvallisuuden toteuttamista valvotaan. Turvallisuustoiminnan toteuttaminen on osana virkavastuuta. Valvonnan tuloksia ei ole dokumentoitu.

A 105.0	Huomioiko turvallisuuspolitiikka yleisen lainsäädännön ja paikallisten turvallisuusmääräysten sisältämät velvoitteet?	Turvallisuustoimintaa koskeva lainsäädäntö tunnetaan ja lainsäädännön vaatimukset on huomioitu turvallisuusohjeissa. Turvallisuuslainsäädännön seuraaminen on määritetty organisaation tehtävänkuvauksessa henkilön tai toiminnon tehtäväksi.		Lainsäädännön vaatimukset tunnetaan teoriatasolla ja ne tiedostetaan hyvin. Tästä huolimatta yksikön pelastussuunnitelmaa ei ole päivitetty ajan tasalle uuden pelastuslain kanssa. Turvallisuuslainsäädännön seuraamiselle on määritetty vastuuhenkilö. Vastuuhenkilö saa vuosittain täydennyskoulutusta turvallisuuslainsäädännön muutoksista.
A 105.1	Pääkysymys: Onko toiminnan lakisääteiset vaatimukset huomioitu? Lisäkysymkset: Miten lakisääteisiä vaatimuksia seurataan ja miten ne huomioidaan toiminnassa? Ovatko esimerkiksi henkilötietojen käsittelyn prosessit henkilötietolain edellyttämällä tasolla?	1) Toimintaa koskevat laki- ja sopimusperustaiset vaatimukset on tunnistettu ja täytetty. 2) Kansallisten turvaluokiteltujen aineistojen luokittelu, jakelu ja käsittely toteutetaan kansallisten käsittelysääntöjen, aineiston asettamien vaatimusten, ja/tai erillisen sopimuksen mukaisesti. 3) Kansainvälisten turvaluokiteltujen aineistojen luokittelu, jakelu ja käsittely toteutetaan kansainvälisten sopimusten, aineiston asettamien vaatimusten, ja/tai erillisen sopimuksen mukaisesti.		Lakisääteiset vaatimukset huomioidaan ja tiedostetaan. Henkilökunnan tietoisuuteen niitä jalkautetaan kuitenkin huonosti. Esimerkiksi uudelle työntekijälle ei ole annettu lainkaan tietoturvakoulutusta.
A 106.0	Pääkysymys: Onko turvallisuuspolitiikan sisältö tiedotettu kaikille työntekijöille, jotta heillä on selvä kuva omista turvallisuuteen liittyvistä velvollisuuksistaan ja vastuistaan? Lisäkysymys: Onko turvallisuuspolitiikkadokumentaatio jatkuvasti kaikkien saatavilla?	Turvallisuuspolitiikka on koulutettu koko henkilöstölle. Koulutus on dokumentoitu. Koulutus kerrataan esimerkiksi osana muuta koulutusta. Politiikka on helposti kerrattavissa esimerkiksi tietojärjestelmän tai ilmoitustaulun avulla. Organisaation turvallisuuspolitiikka on koulutettu tarvittaville sidosryhmien edustajille.		Turvallisuuspolitiikkaa ohjaava dokumentaatio on jatkuvasti saatavilla. Dokumentaation saatavuudesta ja päivityksestä ei tiedoteta työntekijöille riittävästi. Turvallisuusdokumentaatioiden sisältöä ei kerrata muun koulutuksen yhteydessä.
A 107.0	Sisältääkö organisaation turvallisuuspolitiikka vaatimuksen kaikkien työntekijöiden sitoutumisesta jatkuvaan turvallisuustilanteen parantamiseen?	Turvallisuuspolitiikka sisältää henkilökohtaisen sitoutumisen merkityksen.		Turvallisuuspolitiikan dokumentaatiossa ei ole sitoutettu erikseen vaatimusta turvallisuustilanteen parantamiselle. Lainsäädännön puolelta löytyy kuitenkin toimintavelvoite turvallisuuden ylläpitämiseen.

A 108.0	Onko turvallisuuspolitiikassa määritetty organisaation keskeiset turvallisuustavoitteet?	Keskeiset turvallisuustavoitteet on kuvattu turvallisuuspolitiikassa.		Turvallisuuspolitiikkaan on määritelty lakisääteiset turvallisuuskoulutusvelvoitteet. Organisaation tulostavoitteissa on määritelty osittaisia tavoitteita työturvallisuuden osalta.
A 201.0	Onko organisaatiolla kirjoitettu ja dokumentoitu toimintaohjelma turvallisuuden johtamiseksi ja turvallisuustyön tavoitteiden saavuttamiseksi?	Organisaatiolla on toimintaohjelma, joka kattaa turvallisuusjohtamisen, henkilöstö-, tieto- ja tilaturvallisuuden kehittämisalueet. Toimintaohjelma on erillinen dokumentti tai osa organisaation toimintasuunnitelmaa.		Pelastussuunnitelma ja turvallisuussuunnitelma löytyvät, mutta niitä ei ole päivitetty uuden pelastuslain tasalle. Myös osa suunnitelmiin sisällytetyistä vastuuhenkilöistä ovat jo jääneet eläkkeelle tai muuten vaihtuneet. Turvallisuussuunnitelmat eivät ole osana yksikön toimintasuunnitelmaa. Johdon tasolla kuitenkin ymmärretään, että toimintaohjelma tulisi liittää yksikön vuosittaiseen toimintasuunnitelmaan.
A 202.0	Onko toimintaohjelmassa eritelty menetelmät, vastuut ja aikataulut tavoitteiden saavuttamiseksi?	Organisaatiolla on turvallisuuden toimintaohjelma, jossa on kuvattu ainakin turvallisuusjohtamisen, henkilöstö-, tieto- ja tilaturvallisuuden kehittämisalueiden osalta vaadittavat tavoitteet, vastuut ja aikataulut. Toimintaohjelma on erillinen dokumentti tai osa organisaation toimintasuunnitelmaa.		Suunnitelmiin ei ole asetettu tavoitteita, vastuita tai aikatauluja.
A 203.0	Tarkistetaanko toimintaohjelma säännöllisesti?	Ohjelman tarkistaminen on osa jatkuvaa johtamiskäytäntöä.		Pelastussuunnitelman osalta näkyy päivämäärämerkintöjä, joiden voisi viitata tarkistamiseen. Tarkistaminen ei ole kuitenkaan johtanut sellaisiin toimenpiteisiin, jotka päivittäisivät suunnitelman vaatimustenmukaiseksi.

A 204.0	Onko organisaatiolla dokumentoitu ohjelma tietoturvallisuuden johtamiseksi ja turvallisuustyön tavoitteiden saavuttamiseksi?	Organisaatiolla on tietoturvasuunnitelma, toimintaohje, tai vastaava, ja siihen liittyvät ohjeet tarpeen mukaan. Vaaditaan, että 1) suunnitelma sisältää kuvaukset ainakin hallinnollisesta, fyysisestä ja tietoteknisestä tietoturvallisuudesta; 2) suunnitelma ottaa huomioon mahdollisen toimintaa säätelevän lainsäädännön (ml. tietosuoja); 3) suunnitelmaan liittyvät ohjeet ovat riittäviä suhteessa organisaatioon ja suojattavaan kohteeseen.		Tietoturvasuunnitelma on nimellisesti mukana pelastussuunnitelmassa, mutta on sisällöltään vaatimaton. Vaatimustenmukaista suunnitelmaa ei ole olemassa yksikkötasolla. Teknistä tietoturvallisuutta toteuttaa erillinen virasto, jolla on omat ohjeistuksensa yksikön tietoturvallisuuden toteuttamiseksi.
A 301.0	Onko organisaation liiketoiminta ja sitä tukeva turvallisuuspolitiikka ja -ohjelma perusteena turvallisuustyön tavoitteita asetettaessa?	Turvallisuustyön tavoitteet on asetettu politiikan mukaisesti, selkeästi ja mitattavasti.		Tavoitteet ovat osa viranomaisyksikön toimintaa ja toimintavelvoitetta.
A 302.0	Onko organisaatio asettanut turvallisuustavoitteet organisaation eri hierarkiatasoille ja/tai toiminnoille?	Organisaatiolla on selkeät ja dokumentoidut turvallisuustavoitteet, jotka kattavat ohjelman mukaiset turvallisuuden osa-alueet ja eriteltynä organisaation tarvittavat osat ja tasot.		Dokumentoidut suunnitelmat ovat yleisohjeita, mutta eri sidosryhmissä otetaan huomioon erilaiset turvallisuustavoitteet ja -tarpeet. Sidosryhmiä koskevia erittelyjä ei ole dokumentoitu.
A 303.0	Onko tavoitteet asetettu siten, että niiden saavuttaminen on mitattavissa?	Turvallisuustoiminnan tavoitteet on asetettu konkreettisesti ja mitattavasti.		Tavoitteita ei ole asetettu konkreettisesti ja mitattavasti. Dokumentoinnissa on selkeitä puutteita.
A 304.0	Onko tavoitteiden saavuttamiselle asetettu aikataulu?	Tavoitteiden saavuttamiselle on asetettu aikataulu.		Tavoitteille ei ole asetettu aikataulua.

A 305.0	Onko seuraavat tekijät otettu huomioon tavoitteiden asettamisen yhteydessä: a. tunnistetut riskit b. organisaation oman toiminnan ja/tai liiketoiminnan vaatimukset c. tekniset vaatimukset ja mahdollisuudet d. taloudelliset vaatimukset e. muiden intressiryhmien vaatimukset (esim. asiakkaat, viranomaiset) f. lainsäädännön ja/tai muiden ohjeistojen sekä sopimusten vaatimukset	Asetettavat tavoitteet sisältävät tarvittavilta osin kuvauksen liittymisestä tunnistettuihin riskeihin, teknisiin ja taloudellisiin vaatimuksiin sekä mahdollisuuksiin, organisaation oman toiminnan ja/tai liiketoiminnan vaatimuksiin, muiden intressiryhmien vaatimuksiin ja/tai lainsäädännön/muiden ohjeistojen vaatimuksiin huomioiden tekijät a), b), c), e), f).		Riskejä ei arvioida kokonaisvaltaisesti eikä johdetusti. Ne perustuvat lähinnä tilanne- ja tapauskohtaisiin arviointeihin. Riskien arviointia ollaan päivittämässä. Taloudellisten syiden takia turvallisuustoimintaa ei pysty suorittamaan vaatimustenmukaisesti, jonka vuoksi muun muassa yksikön turvallisuustekniikka on osin vanhentunutta.
A 306.0	Onko koko suojattavan tiedon käsittely-ympäristö suojattu organisaation tietoturvaperiaatteiden ja tiedon merkityksen/luokituksen mukaisesti? Lisäkysymykset: Kattavatko suojaukset kaikki loogisesti kytketyt tietoverkot ja -järjestelmät, joissa suojattavaa tietoa käsitellään? Kattavatko suojaukset myös sellaiset tietoverkot ja -järjestelmät, joihin tietoa viedään tai joista tietoa tuodaan ilmaraon yli esimerkiksi USB-muisteilla?	Kaikki suojaustason III tiedon käsittely-ympäristöt on suojattu vähintään viranomaisvaatimusten mukaisesti.		Organisaatiotasolla on olemassa yksityiskohtaisia ohjeistuksia tietojen käsittelyyn. Yksikkötasolla tietoturvakäytäntöjen noudattaminen, kouluttaminen ja toteuttaminen ovat puutteellista ja hajanaista. Teknistä tietoturvallisuutta hoidetaan organisaatiossa erillisen viraston ohjauksessa.
A 401.0	Onko organisaatiolla menetelmät tunnistaa ja arvioida turvallisuusriskit?	Organisaatio arvioi turvallisuuden kokonaisuuteen liittyvät riskit ja riskienarviointi on turvallisuustyön tärkeysjärjestyksen peruste. Menettelytapa on säännöllinen ja tulokset dokumentoidaan.		Turvallisuusriskejä ei arvioida säännöllisesti. Riskejä arvioidaan tapauskohtaisesti, mutta ne eivät perustu riskianalyysimenetelmiin eikä niitä dokumentoida.

A 401.1	Pääkysymys: Onko toiminnalle tärkeät suojattavat kohteet (toiminnot, tiedot, järjestelmät, prosessit) tunnistettu? Lisäkysymykset: Mitä uhkia niihin kohdistuu? Onko suojattaville kohteille määritetty vastuuhenkilöt?	1) Suojattavat kohteet (assets) on tunnistettu. 2) Suojattaviin kohteisiin kohdistuvat uhat on tunnistettu. 3) Suojattaville kohteille on nimetty omistaja/ vastuuhenkilö. 4) Suojattavien kohteiden suojausmenetelmät on suhteutettu kohteisiin sekä niihin kohdistuviin riskeihin (vrt. A 401.2).		Suojattaville kohteille on määritelty vastuuhenkilöt, mutta ne eivät ole ajan tasalla. Tärkeät kohteet on tunnistettu, mutta tunnistusprosessia ja sen tuloksia ei dokumentoida.
A 401.2	Miten suojattaviin kohteisiin kohdistuvia riskejä arvioidaan?	1) Suojattaviin tietoihin kohdistuvia riskejä hallitaan prosessina jollain järjestelmällisellä menetelmällä. 2) Em. prosessissa on määritelty tunnetut turvallisuusriskit ja turvatoimet niiden vähentämiseksi hyväksyttävälle tasolle. 3) Turvatoimien tehokkuutta arvioidaan vähintään vuosittain ja lisäksi merkittävien muutosten yhteydessä. 4) Turvallisuusriskien hallinta on erottamaton osa suojattavan kohteen viestintä- ja tietojärjestelmien määrittelyä, kehittämistä, käyttöä ja ylläpitoa. 5) Johto ja tiedon omistajat ovat hyväksyneet valitut suojausmenetelmät ja jäännösriskit.		Riskejä ei arvioida yksikössä järjestelmällisesti eikä kokonaisvaltaisesti. Yksiköstä erillinen, teknistä tietoturvallisuutta ohjaava ja koordinoiva virasto vastaa tietojärjestelmien riskien tunnistamisesta ja teknisistä tietoturvallisuusriskeistä.
A 402.0	Kattavatko nämä menetelmät normaalin toiminnan, erityistilanteet, onnettomuudet ja hätätapaukset? Otetaanko aliurakoitsijat ja palveluntarjoajat huomioon?	Riskienarviointi kattaa ainakin turvallisuusjohtamisen sekä henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet. Asiat on huomioitu myös normaalitoiminnasta poikkeavien tilanteiden ja tarvittavien sidosryhmien osalta.		Suojattavien kohteiden riskejä hallitaan aliurakoitsijoista ja palveluntarjoajista tehdyllä suppealla turvallisuusselvityksellä. Poikkeavissa tilanteissa riskien arviointia pidetään jatkuvasti ajan tasalla. Poikkeaviin tilanteiden riskien arviointi on koulutettu esimiestasolla ja siihen on olemassa ohjeistus.

A 403.0	Dokumentoidaanko riskienarviointien tulokset ja päivitetäänkö ne säännöllisesti?	Riskienarviointi tehdään vähintään vuosittain ja organisaation tilanteen muuttuessa siten, että on tarkoituksen mukaista päivittää tehty arvio. Riskienarvioinnit dokumentoidaan siten, että ne ovat todennettavissa.		Riskienarviointien tuloksia ei dokumentoida eikä päivitetä.
A 404.0	Otetaanko riskienarviointien havainnot huomioon turvallisuustoiminnan tavoitteita asetettaessa?	Riskienarvioinnin tulokset on huomioitu turvallisuustoiminnan tavoitteita asetettaessa.		Riskejä arvioidaan hajanaisesti ja tapauskohtaisesti. Mikäli tapauskohtainen riskienarviointi tehdään, se otetaan huomioon organisaation tavoitteissa. Tavoitteiden toteuttamisessa on kuitenkin puutteita talousresurssien puutteiden vuoksi.
A 405.0	Voidaanko riskienarvioinnin tulosten perusteella priorisoida riskit?	Riskienarvioinnin tuloksena riskit luokitellaan tärkeysjärjestykseen.		Riskejä ei arvioida säännöllisesti.
A 406.0	Antavatko riskienarvioinnit perusteet turvallisuuskoulutuksen vaatimuksille?	Riskienarviointien tulokset vaikuttavat suunnitellun koulutuksen sisältöön. Koulutus tunnistetaan yhtenä keinona vaikuttaa riskien hallintaan.		Riskien arviointi ei ole järjestelmällisesti dokumentoitua. Koulutus muodostuu kuitenkin sellaiseen riskien arviointiin, jota käydään kouluttajien välisen keskustelun tasolla. Koulutuksen lisääminen kohonneessa turvallisuusriskissä perustuu lähinnä yksittäisten toimijoiden aktiivisuuteen.
A 407.0	Onko organisaatiolla menetelmät valvoa turvallisuuden riskienarviointien perusteella tehtyjen toimenpiteiden toteuttamista ja tehokkuutta?	Turvallisuusjohtamisen prosessi sisältää riskienarvioinnin perusteella tehtyjen toimenpiteiden toteuttamisen ja tehokkuuden arvioinnin.		Menetelmiä ei ole. Tehokkuutta arvioidaan tapaus- ja tilannekohtaisesti.
A 408.0	Pääkysymys: Miten organisaation tietoturvallisuutta arvioidaan? Lisäkysymys: Kehitetäänkö toimintaa havaintojen perusteella?	1) Suojattavan kohteen tietoturvallisuuden arviointiin ja mittaamiseen on käytössä järjestelmällinen menetelmä. 2) Suojattavan kohteen turvallisuudelle suoritetaan riippumaton katselmus suunnitelluin väliajoin, ja lisäksi aina, kun turvallisuuden toteuttamisessa tapahtuu merkittäviä muutoksia.		Tietoturvallisuuden arviointi ja mittaaminen eivät ole järjestelmällistä. Tietoturvallisuutta korostetaan ja siihen puututaan lähinnä tietoturvarikkomusten jälkeisissä jälkipuinneissa. Ennalta ehkäisevää toimintaa tietoturvarikkomusten varalta ei ole jalkautettu kentälle, vaikka ohjeita löytyykin runsaasti.

A 409.0	Miten tietoturvallisuudesta on huolehdittu alihankinta-, palveluhankinta- ja muussa vastaavassa yhteistyössä?	Suojaustason III aineistoa ei luovuteta alihankkijalle tai vastaavalle ilman viranomaisen etukäteissuostumusta.		Tietoturvaperehdytyksen sekä palveluntarjoajiin kohdistuvien turvallisuusselvitysten kautta pyritään ennalta ehkäisemään mahdollisia rikkomuksia. Turvallisuusselvitykset ovat palveluntarjoajiin pääasiassa suppeita turvallisuusselvityksiä, joten niiden perusteella tietoturvaan kohdistuvia riskejä ei pysty kattavasti arvioimaan. Henkilökuntaa kehotetaan yleisesti käsittelemään suojattavaa aineistoa vaatimustenmukaisella tavalla. Käytännön ohjeistusta tai dokumentointia ei tähän ole kuitenkaan yksikkötasolla olemassa.
A 410.0	Miten organisaatiossa toimitaan tietoturvapoikkeamatilanteissa? Lisäkysymys: Miten tietoturvapoikkeamien hallinta on käytännössä toteutettu?	Tietoturvapoikkeamien hallinta on 1) suunniteltu, 2) ohjeistettu/koulutettu, 3) dokumentoitu käyttöympäristöön nähden riittävällä tasolla, ja erityisesti 4) viestintäkäytännöt ja -vastuut on sovittu. 5) harjoiteltu 6) Tapahtuneesta tai epäillystä tietoturvapoikkeamasta ilmoitetaan välittömästi turvallisuusviranomaiselle tai viranomaisen erikseen hyväksymälle taholle.		Ohjeita tietoturvapoikkeamatilanteisiin lähetetään henkilöstölle erillisinä ohjeina sähköisessä muodossa. Ohjeistukset eivät tule konkreettisesti ilmi eikä niitä harjoitella.
A 501.0	Ovatko turvallisuustyön vastuut määritetty? Kattavatko määrittelyt organisaation eri tasot?	Turvallisuusorganisaatio kattaa turvallisuusjohtamisen sekä henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet. Vastuulliset henkilöt on nimetty ja koulutettu ja tehtävä on osa henkilön toimenkuvausta.		Turvallisuuden osa-alueisiin on nimetty henkilöt ja vastuu on määritelty henkilön tehtävänkuvauksessa. Vastaavia henkilöitä koulutetaan omaan vastuualueeseensa. Tällä hetkellä yksiköltä puuttuu tietoturvavastaava. Turvallisuusorganisaation näkyvyys on kuitenkin heikkoa. Yksikön uusi työntekijä ei osannut tunnistaa johtamisjärjestelmää.
A 501.1	Onko organisaation tietoturvallisuudella johdon tuki? Miten tuki käytännössä näkyy organisaation toiminnassa?	Organisaation tietoturvallisuudella on johdon tuki. Vaaditaan vähintään, että 1) tietoturvallisuus on vastuutettu (johdon vastuut, tietohallinnon / järjestelmien ylläpidon vastuut, peruskäyttäjän vastuut, jne.); 2) organisaatiolla on johdon hyväksymät tietoturvaperiaatteet ja -käytänteet;		Johto ymmärtää tietoturvallisuuden olevan tärkeänä osa organisaation kokonaisturvallisuutta. Käytännössä johdon osuus tietoturvallisuusjohtamisessa jää piiloon eikä sitä huomaa konkreettisella tasolla muuten kuin mahdollisen lisäkoulutuksen tarpeen huomioimisella.

		3) tietoturvaperiaatteet ja -käytänteet on saatettu koko organisaation tietoon; 4) tietoturvaperiaatteet ja -käytänteet katselmoidaan vuosittain ja aina, kun merkittäviä muutoksia tapahtuu; 5) johto edellyttää, että työntekijät, toimittajat ja ulkopuoliset tietojen käsittelijät toimivat organisaation tietoturvaperiaatteiden mukaisesti; 6) tietoturvallisuudelle on varattu toimintavaatimuksiin nähden riittävät resurssit.		
A 502.0	Ovatko roolit, vastuut ja toimeenpanovalta tiedotettu organisaatiossa ja niille ulkopuolisille tahoille, joiden on tunnettava turvallisuusorganisaation rakenne?	Turvallisuusorganisaatio on koulutettu henkilöstölle ja tieto on saatavissa päivitettynä esimerkiksi tietojärjestelmän tai ilmoitustaulun avulla.		Turvallisuusorganisaation rakenteesta tiedotetaan. Tiedottamisen ja kouluttamisen taso vaihtelee hyvin paljon. Perehdytysvaiheessa turvallisuusorganisaation rakenteesta ei kerrota tarpeeksi selvästi ja siitä selvyyden saaminen edellyttää työntekijän omatoimisuutta.
A 503.0	Onko turvallisuustyölle suunnattu riittävästi resursseja työn toteuttamiseksi, kontrolloimiseksi sekä parantamiseksi? Resurssien tulisi kattaa: - henkilöstö - erityisosaaminen - teknologiset resurssit - taloudelliset resurssit	Turvallisuustyöstä vastaa koulutettu ja kokenut henkilöstö, jonka osaamistasoa ylläpidetään suunnitellusti ja jatkuvasti. Turvallisuusjohtaminen kattaa mm. henkilöstön, teknologian ja taloudellisten resurssien riittävyyden arvioinnin. Osatekijät on sisällytetty osaksi turvallisuustyön jatkuvaa parantamista.		Teknologiset resurssit ovat puutteellisia. Turvallisuuskriittisillä työalueilla henkilöstöresurssit ovat vähäistä. Turvallisuustyöstä vastaavia kuitenkin koulutetaan hyvin omille osa-alueilleen ja vaadittava pohjakoulutus tiettyihin tehtäviin edellyttää normaalia kattavampaa turvallisuuskoulutusta.
A 504.0	Onko organisaation ylin johto määrittänyt henkilön, joka on vastuussa turvallisuustoiminnan kehittämisestä ja johtamisesta sekä siitä, että turvallisuustyö kattaa kaikkien organisaation tasojen tarpeet?	Organisaatiolla on turvallisuudesta keskitetysti vastaava henkilö, jolla on riittävät mahdollisuudet johtaa ja koordinoida turvallisuustoimintaa ja hallita ainakin henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet.		Yksiköllä on ylimpään johtoon kuuluva henkilö, joka vastaa turvallisuustoiminnan strategisesta johtamisesta. Hänen alaisuudessaan toimii esimies, jonka työnkuvanaan on turvallisuustoiminnan operatiivinen vastuu. Tietoturvan teknisestä osa-alueesta vastaa yksikön ulkopuolinen virasto.

A 505.0	Onko nimetyllä turvallisuustyöstä vastaavalla henkilöllä vastuu ja valtuus sen varmistamiseksi, että turvallisuuden johtamisjärjestelmä on muodostettu niiden vaatimusten mukaisesti, joita tavoitteissa on asetettu?	Turvallisuudesta vastaava henkilö on organisaatiossa sellaisella tasolla, että hänellä on mahdollisuus vaikuttaa turvallisuuden johtamisjärjestelmän kokonaisuuteen. Vaikuttamismahdollisuus on yksilöitävä organisaation prosessikuvauksessa ja/tai henkilön tehtävänkuvauksessa.		Kohteen ylin johto vastaa hallinnollisen turvallisuuden toteuttamisesta. Turvallisuudesta vastaavan esimiehen tehtävänkuvauksessa on yksilöity vaikutusmahdollisuus turvallisuustoiminnan kehittämiseen ja johtamiseen.
A 506.0	Onko organisaation johto sitoutunut turvallisuustavoitteisiin ja niiden saavuttamiseen sekä turvallisuuden jatkuvaan parantamiseen?	Organisaation johto on mukana turvallisuustyön tavoitteiden asettamisessa, menetelmien valinnassa ja tavoitteiden seurannan arvioinnissa. Malli on yksilöitävä organisaation prosessikuvauksessa.		Ylin johto sitoutuu tavoitteiden saavuttamiseen.
A 601.0	Onko organisaatiolla jatkuvuudenhallintamenettely?	Organisaation toiminnan johtamisessa on otettu huomioon varautuminen liiketoimintaa vaikeuttaviin tai katkaiseviin häiriötilanteisiin ja laadittu niitä koskevat valmius- ja toipumissuunnitelmat organisaation keskeisimpiin toimintoihin. Resurssitarve on määritetty ja niiden saatavuus suunniteltu. Jatkuvuuden hallinnan toteutumista seurataan ja arvioidaan.		Yksiköllä on jatkuvuudenhallintamenettely liiketoimintaa vaikeuttaviin tai katkaiseviin häiriötilanteisiin.
A 602.0	Onko organisaatiossa määritetty onnettomuuksien, vaaratilanteiden ja turvallisuuspoikkeamien käsittelystä ja tutkinnasta vastaavat henkilöt?	Organisaatio on määrittänyt poikkeamatilanteiden johtamisen osana turvallisuuden organisointia. Vastuut on kuvattu henkilöiden tehtäväkuvauksissa. Vastaavat henkilöt ovat hyvin selvillä organisaation ja viranomaisen välisestä toimivalta- ja vastuujaosta.		Yksikkö on määrittänyt henkilöt, jotka vastaavat poikkeamatilanteisiin varautumisesta, suunnittelusta ja niihin kouluttamisesta.

A 603.0	Onko vastuut kriisitilanteiden, onnettomuuksien, vaaratilanteiden ja turvallisuuspoikkeamien vaikutusten ennalta pienentämiseksi määritetty?	Organisaatio on määrittänyt poikkeamatilanteiden johtamisen osana turvallisuuden organisointia. Valtuudet ja vastuut on kuvattu henkilöiden tehtäväkuvauksissa.		Vastuut ovat määritetty ja ne ovat osa yksikön perustehtävää.
A 604.0	Onko organisaatiolla menetelmät turvallisuuspoikkeamien havaitsemiseksi ja suojaavien sekä korjaavien toimenpiteiden tekemiseksi?	Organisaatiossa on tunnettava tapa raportoida turvallisuuspoikkeamat. Turvallisuuspoikkeamien esiintymistä on valvottava.		Yksiköllä on tekniset valmiudet havainnoida turvallisuuspoikkeamia (palohälytys-, murtohälytys- ja kameravalvontajärjestelmät). Henkilökunta raportoi turvallisuuspoikkeamista suullisesti ja osittain sähköpostin välityksellä. Raportoiminen tilannesidonnaista. Poikkeamien dokumentoinnissa parantamisen varaa.
A 605.0	Onko organisaatiolla menetelmät sen varmistamiseksi, että tehdyt suojaavat ja korjaavat turvallisuustoimenpiteet ovat tehokkaita ja oikein kohdistettuja?	Turvallisuustoimenpiteiden toivottua ja saavutettua vaikutusta verrataan. Organisaatiolla on käsitys panos-tuotos -suhteesta.		Yksikön panos-tuotos suhde on tapauskohtainen. Turvallisuustoimenpiteet pyritään toteuttamaan mahdollisimman tehokkaasti ja taloudellisesti.
A 606.0	Onko organisaatiolla menetelmät arvioida riskit, joita suunnitellut korjaavat toimenpiteet aiheuttavat?	Turvallisuustoiminnan prosessi sisältää arvion muutosten negatiivisista vaikutuksista.		Riskien arviointi ei ole järjestelmällistä. Arvioinnit perustuvat yksittäisiin tapauksiin.
A 607.0	Onko organisaatiolla menetelmät turvallisuustoimenpiteiden vaikutusten analysointia varten?	Organisaatio analysoi turvallisuustoimenpiteiden vaikutukset vähintään vuosittain. Esimerkiksi tilastoja seuraamalla tarkastellaan tietyn vaaratilanteen tapahtumataajuuden muutosta.		Tilastoja analysoidaan enemmälti henkilöstö- ja työturvallisuuden osa-alueilla. Muiden turvallisuuden osa-alueilta ei ole dokumentoitua seurantaraporttia.
A 608.0	Onko organisaatiossa menettely, jonka avulla varmistetaan, että merkittävät tietojenkäsittely-ympäristön muutokset tapahtuvat hallitusti?	Tietojenkäsittelyyn liittyviin muutoksiin on käytössä muutoshallintamenettely.		Teknisiä muutoksia hallitaan ulkopuolisen tietoturvaa organisoivan viraston kautta. Muutosten hallinta ei ole niinkään johdettua, vaan on riippuvaista henkilön omasta aktiivisuudesta. Virallinen ohjeistus jaetaan kirjallisesti, mutta käytännön koulutus on pääasiassa sellaisen henkilön varassa, joka on asioihin perehtynyt.

A 701.0	Onko organisaatiolla toimintamallit, jotka koskevat: a. turvallisuustiedostoja /turvallisuusrekistereitä tai dokumentointimenetelmiä? b. turvallisuusdokumentaation tietojen yksilöintiä ja jäljittämistä? c. turvallisuusdokumentaation säilyttämisaikoja, säilytyspaikkaa ja säilytyksen vastuita?	Organisaatiolla on järjestelmä, joka sisältää turvallisuusrekisterit, omat ohjeistot ja tapahtuneet turvallisuuspoikkeamat. Järjestelmä täyttää lainsäädännön asettamat vaatimukset (mm. rekisteriseloste).		Turvallisuusdokumentteja säilytetään niille kuuluvassa paikassa kirjallisena ja niitä on saatavissa myös sähköisenä yksikön sisäisestä verkosta. Rekisteriselosteet puutteellisia.
A 702.0	Sisältävätkö rekisterit myös tiedot turvallisuustavoitteiden saavuttamisen tasosta?	Organisaatio pystyy osoittamaan turvallisuustavoitteiden saavuttamisen tason vähintään vuosittain.		Turvallisuustavoitteita ei aseteta kokonaisturvallisuudelle, joten seurantatilastoja ei ole saatavilla.
A 703.0	Sisältävätkö turvallisuusrekisterit tiedot annetuista turvallisuuskoulutuksista?	Organisaatiolla on koulutusrekisteri, jolla voidaan osoittaa annettu koulutus, sen sisältö ja voimassaolo.		Turvallisuuskoulutukset ovat dokumentoitu.
A 704.0	Voidaanko dokumentaation perusteella osoittaa, että turvallisuuskoulutuksen taso on riittävän korkea?	Organisaation koulutusrekisteriin on kirjattu tasovaatimukset ja niiden toteutuminen varmistetaan siten, että työtehtävää ei aloiteta ennen koulutusvaatimuksen täyttymistä.		Turvallisuuskoulutukseen ei ole säädetty tasovaatimuksia. Vaatimusten täyttymistä kuitenkin seurataan kouluttajien taholta.
A 801.0	Ovatko organisaation kaikki henkilöt tietoisia turvallisuusvaatimusten noudattamisen tärkeydestä ja oikeista toimintatavoista?	Organisaation koko henkilöstö on koulutettu henkilöstö-, tila- ja tietoturvallisuuden vaatimuksien osalta. Projektihenkilöstö on koulutettu projektikohtaisten vaatimusten mukaisesti.		Henkilökuntaa ei ole koulutettu kokonaisvaltaisesti. Koulutus hajanaista.
A 802.0	Onko varmistuttu siitä, että henkilöstö tuntee omaan työhönsä liittyvät turvallisuusriskit?	Riskienarvioinnin yhteydessä käsitellään ainakin henkilöstö-, tila- ja tietoturvallisuuden osa-alueita koskevat seikat. Henkilöstölle selvitetään sen tehtäviin liittyvät turvallisuusriskit.		Turvallisuusriskejä käydään läpi perehdytysvaiheessa ja henkilöstön koulutuksessa. Tiettyjen henkilöstöryhmien pohjakoulutukseen kuuluu turvallisuusriskeihin perehtyminen.

A 803.0	Onko varmistuttu siitä, että henkilöstö osaa toimia oikein tilanteissa, joissa turvallisuus on vaarantunut?	Organisaatiolla on tiedossaan sitä uhkaavat keskeiset turvallisuusriskit. Tärkeimpiin poikkeamatilanteisiin on dokumentoidut toimintamallit ja niistä keskeisimpiä harjoitellaan säännöllisesti.		Dokumentoidut toimintamallit ovat olemassa. Poikkeamatilanteita ei harjoitella säännöllisesti.
A 803.1	Miten organisaatiossa valvotaan tietoturvaohjeiden noudattamista? Lisäkysymys: Onko tietoturvarikkomusten käsittely ja seuraukset määritelty?	1) Tietoturvaohjeiden noudattamista valvotaan ja rikkeisiin puututaan. 2) Tietoturvarikkomusten käsittely ja seuraukset on määritelty. 3) Käsittely ja seuraukset ovat samat koko henkilöstölle. 4) Tietoturvarikkomukset tutkitaan viranomaistoimenpitein.		Tietoturvarikkomuksia seurataan yksikköä ylemmällä organisaatiotasolla. Mikäli tietoturvarikkeitä kuitenkin havaitaan, niihin pyritään puuttumaan. Virkamieslaissa on rikkeiden käsittelystä ja seurauksista omat määrittelynsä.
A 804.0	Onko organisaatiolla menetelmä varmistua siitä, minkä tasoista turvallisuuskoulutusta henkilöstö tarvitsee tehtävissään?	Organisaatiolla on toiminto, joka määrittää turvallisuuskoulutuksen tasovaatimukset ainakin henkilöstö-, tila- ja tietoturvallisuuden osa-alueiden osalta.		Tilaturvallisuuden osalta tasovaatimuksia on suunniteltu. Tieto- ja henkilöstöturvallisuuden osalta ei ole toimintoa.
A 805.0	Onko organisaatiolla menetelmä varmistaa, että työntekijöillä on tehtävien edellyttämä sopivuus, turvallisuuskoulutus, tehtävään perehtyminen ja kokemus?	Turvallisuuskoulutusrekisteristä saadaan tieto tehtävän edellyttämästä turvallisuuskoulutustasosta.		Rekisterissä ei mainintaa tasovaatimuksista. Yksikön turvallisuuskouluttajilla on kuitenkin vahva käsitys tehtävien vaatimustenmukaisuudesta
A 806.0	Miten organisaatiossa on huolehdittu riittävästä ohjeistuksesta, koulutuksesta ja tiedotuksesta?	Organisaatiossa on huolehdittu riittävästä ohjeistuksesta ja koulutuksesta. 1) Henkilöstö on saanut perehdytyksen yhteydessä ohjeet kuinka toimia organisaation turvaperiaatteiden mukaisesti. Ohjeistuksen/ koulutuksen tulee sisältää tärkeimmät toimintatilanteet (peruskäyttö, etäkäyttö, matkatyö, ylläpito, jne.) ja -tavat. 2) Henkilöille, jotka on otettu palvelukseen sellaiseen asemaan, jossa he voisivat		Henkilöstön perehdytys on vaillinaista turvallisuuskoulutuksen osalta. Tietoturvapoikkeamista ei tiedoteta organisaatiotasolla.

päästä suojattaviin tietoihin, annetaan heti aluksi ja säännöllisin väliajoin tarkat ohjeet turvatoimien tarpeellisuudesta ja niiden täytäntöönpanomenettelyistä.
3) Suojattavia tietoja käsitteleviin järjestelmiin on laadittu turvallisen käytön ohjeistus.
4) Tiedon merkitsemistä (luokittelua), käsittelyä (sis. salaus) ja tallennusta koskeva ohjeistus on laadittu ja otettu käyttöön.
5) Henkilöstö on ohjeistettu ja velvoitettu ilmoittamaan havaitsemistaan tietoturvapoikkeamista ja -uhista.
6) Tulevista työasemien tietoturva-aukkojen päivityksistä tiedotetaan vähintään sillä tarkkuudella, että käyttäjät ovat tietoisia siitä, mitä toimia heiltä vaaditaan.
7) Käyttäjille tiedotetaan kaikkein merkittävimmistä ajankohtaisista uhista, jotka kohdistuvat organisaation käyttäjiin (esim. kohdistetuista hyökkäyksistä).
8) Järjestelmien ylläpitohenkilöstö on suorittanut ko. järjestelmiä koskevan valmistaja-/ ympäristökohtaisen turvallisuuskoulutuksen, muun yleisesti hyväksytyn ko. ympäristöön soveltuvan turvallisuuskoulutuksen, tai ylläpitohenkilöstölle on muuten hankittu riittävä osaaminen ko. järjestelmien turvalliseen ylläpitoon. Henkilöille annettava turvallisuuskoulutus on dokumentoitu.

A 807.0	Onko tietoon ja tietojenkäsittelypalveluihin määritetty hyväksyttävän käytön säännöt ja onko niistä tiedotettu henkilöstölle?	1) Tiedon ja tietojenkäsittelypalveluihin liittyvien suojattavien kohteiden hyväksyttävän käytön säännöt on määritetty. 2) Hyväksyttävän käytön säännöissä otetaan kantaa vähintään siihen, saako organisaation tietojärjestelmiä käyttää henkilökohtaisiin tarpeisiin (sähköposti, levytila, pankkipalveluiden käyttö, jne.). 3) On selkeästi tiedotettu hyväksyttävän käytön säännöistä henkilöstölle. 4) Hyväksyttävän käytön säännöt ovat henkilöstölle helposti saatavilla.		Ohjeita on olemassa, mutta niitä käydään läpi oikeastaan vain sähköpostitasolla eikä sitä jalkauteta konkreettisella tasolla. Tietojen käsittelyyn liittyvää koulutusta ollaan kuitenkin järjestämässä.
A 901.0	Raportoiko turvallisuudesta vastaava henkilö suoraan organisaation ylimmälle johdolle turvallisuuteen liittyvissä asioissa?	Turvallisuudesta vastaava henkilö raportoi organisaation johdolle säännöllisesti siten, että johtoryhmä on selvillä turvallisuustoiminnan ja turvallisuustilanteen tasosta. Huomattavat poikkeamat tai muutokset on voitava raportoida johdolle välittömästi esimerkiksi kriisienhallintamenettelyn kautta.		Turvallisuudesta vastaava raportoi eteenpäin turvallisuuteen liittyviä asioita. Raportointi on myös vuorovaikutteista: organisaation johdosta raportoidaan olennaisia asioita myös turvallisuudesta vastaavalle.
A 902.0	Tarkastaako organisaation ylin johto säännöllisesti (vähintään kerran vuodessa) turvallisuusjärjestelmän toimivuuden?	Turvallisuusasiat esitetään osana organisaation johtamisprosessia laaja-alaisesti ainakin kerran vuodessa johtoryhmälle. Johtoryhmästä on nimetty henkilö, joka seuraa turvallisuuteen liittyviä asioita osana toimenkuvaansa.		Turvallisuusjärjestelmän toimivuutta tarkastellaan jatkuvasti.
A 903.0	Arvioidaanko ylimmän johdon tekemissä tarkastuksissa turvallisuusjärjestelmän soveltuvuus, resurssien riittävyys ja toiminnan tehokkuus?	Organisaation turvallisuustavoitteet ja tavoitteiden saavuttaminen esitetään mitattavassa muodossa.		Turvallisuusjärjestelmän toimivuutta tarkastellaan.

A 904.0	Dokumentoidaanko tehdyt seurantatarkastukset?	Seurantatarkastukset dokumentoidaan.		Tarkastukset ovat osana yksikön jatkuvaa toimintaa, mutta niitä ei dokumentoida. Turvallisuustoimintaan liittyvät palaverit dokumentoidaan ja ovat henkilökunnan nähtävillä.
A 905.0	Toimivatko nämä seurantatarkastukset jatkuvan parannuksen perustekijöinä, eli vaikuttavatko ne politiikan ja tavoitteiden sisältöön?	Turvallisuusjohtamiseen kuuluu prosessi, jossa johdon katselmuksen palautetta käytetään turvallisuuspolitiikan ja – tavoitteiden uudelleenarvioimisessa.		Järjestelmän seuranta on aktiivista ja vaikuttaa turvallisuussuunnitteluun. Turvallisuustoimintaan liittyvien palavereiden tulokset pyrkivät kehittämään turvallisuutta ja puuttumaan turvallisuuspoikkeamiin.